Opinion 11/2020 on the draft decision of the competent supervisory authority of Ireland regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR

Adopted on 25 May 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.

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 GDPR. 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, providing the competent SAs with written guidance explaining the accreditation requirements; and, finally, requesting the competent SAs 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) 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 Irish Supervisory Authority (hereinafter "IE 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 13 February 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 into account 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 IE SA to take further action.

8. This opinion does not reflect upon items submitted by the IE 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 IE 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 supports the development of voluntary compliance activities, including the drawing up of Codes aimed to contribute to the proper application of the GDPR by different sectors of different sizes, and covering processing activities with different levels of risk. In this context, the Board supports the emphasis made by IE SA on the specific needs of micro, small and medium sized enterprises.

11. The Board notes that IE SA introduced a number of examples that in overall help in the interpretation of the draft decision. However, some of the examples are better suited as a requirement, rather than as an example. Therefore, the Board recommends the IE SA to revise the draft accordingly.

12. The Board encourages the IE SA to include in the draft accreditation requirements some examples of the information or documents that applicants have to submit when applying for accreditation.

2.2.2 INDEPENDENCE

13. The Board considers that there are four areas where the monitoring body should demonstrate its independence: 1) legal and decision-making procedures; 2) financial; 3) organisational; 4) accountability.[2] With regards to the IE SA requirements, it seems that the first and the third areas are covered by section 1.1, devoted to 'Structure, Power, and Functions' and the second area is covered by Section 1.2 headed 'Budget and Resources'. However, the Board notices that there is no reference to the fourth area related to accountability.

14. In this regard, the Board notes that the monitoring body should be able to demonstrate "accountability" for its decisions and actions in order to be considered to be independent. The IE 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 personnel about the governance structures and the procedures in place. Thus, the Board recommends the IE SA to introduce the above-mentioned requirements related to accountability of the monitoring body.

15. Regarding section 1.1.2 of the IE SA's draft accreditation requirements, which addresses the issue of internal monitoring body, the Board is of the opinion that independence should exist not only towards the larger entity but with respect to the overall group structure. According to the point 65 of the Guidelines, where an internal monitoring body is proposed, there should be separate personnel and management, accountability and function from other areas of the organisation. This may be achieved in a number of ways, for example, by the use of effective organisational and information barriers and separate reporting management structures for the association and monitoring body. The monitoring body should be able to act free from instructions and shall be protected from any sort of sanctions or interference as a consequence of the fulfilment of its task. In this context, the Board encourages the IE SA to better explain this section and clarify that independence needs to be ensured towards the larger entity, in particular the code owner.

16. As regards section 1.2.1 of the IE SA's draft accreditation requirements, 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. Therefore, the Board recommends that the IE SA amend the explanatory note, adding a reference to such procedures.

17. The Board underlines that the code owners should be able to demonstrate that the proposed monitoring body have adequate resources and personnel to carry out its tasks in an appropriate manner. In particular, resources should be proportionate to the expected number and size of code members, as well as the complexity or degree of risk of the relevant data processing (see paragraph 73 of the Guidelines). The Board notes that in this context, section 1.2.4 of the IE SA's draft requirements lacks some criteria that should be used to measure the adequacy of monitoring body's resources and personnel. Therefore, the Board encourages the IE SA to add some additional details in the draft requirements, such as the expected number and size of code members, as well as the complexity or degree of risk of the relevant data processing.

[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.

18. With regard to the use of sub-contractors, the Board notes that section 1.2.5 of the IE SA's draft accreditation requirements state that "the use of subcontractors does not remove the responsibility of the monitoring body". Indeed, the monitoring body should be the ultimate responsible for all the decisions taken related to its monitoring function. Therefore, the Board encourages the IE 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. In addition, 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. The Board recommends the IE SA to explicitly add this obligation in the draft accreditation requirements.

2.2.3 CONFLICT OF INTEREST

19. The Board recognizes that one of the biggest risks related to the monitoring body is the risk of impartiality. The Board notes that such a risk may arise not only from providing services to the code members but also from a wide range of activities carried out by the monitoring body vis-à-vis code owners (especially in the situation where the monitoring body is an internal one) or other relevant bodies of the sector concerned. In this context, the Board encourages the IE SA to reword the requirement in point 2.1 in more general terms and provide additional clarifications and examples of situations where there is no conflict of interest. Examples could include, among others, services, which are purely administrative or organisational assistance or support activities, which have no influence on the impartiality of the monitoring body.

2.2.4 EXPERTISE

20. With respect to the explanatory note in section 3 of the IE SA's draft accreditation requirements ("Expertise"), the Board notes that, as required by the Guidelines, every code owner has to demonstrate 'why their proposals for monitoring are appropriate and operationally feasible' (see paragraph 41 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. To that end, in order to evaluate the expertise level required by the monitoring body, a code owner should, in general, take into account such factors as: the size of the sector concerned, the different interests involved and the risks of the processing activities addressed by the code. This would also be important if there are several monitoring bodies, as the code will help ensure a uniform application of the expertise requirements for all monitoring bodies covering the same code.

21. With respect to section 3.3 of the IE SA's draft accreditation requirements and the reference to "operational experience, training, and qualifications", in line with the Guidelines (paragraph 69), the Board encourages IE SA to clarify which type of operational experience is required in the text of the requirement itself (i.e. experience in monitoring of compliance, such as in the field of auditing, monitoring, or quality assurance activities).

22. As regards section 3.4 of the IE SA's draft accreditation requirements, the Board considers that it should be better coordinated with sections 3.1, 3.2 and section 3.3, in order to avoid confusion with regard to the scope of section 3.4 in connection with the previous three. Therefore, the Board encourages the IE SA to clarify the relationship between those sections specifying that the monitoring body will have to meet the expertise requirements in sections 3.1, 3.2 and 3.2 in any circumstances, whereas further or specific expertise requirements will only need to be met in case that the code of conduct foresees them.

2.2.5 ESTABLISHED PROCEDURES AND STRUCTURES

23. The Board observes that sections 4.2 and 4.3 of the IE SA's draft accreditation requirements refer to the complexity and risks involved, as part of the criteria to be taken into account in the assessment of the established procedures to monitor compliance of code members with the Code and for the periodic review of the operations of the code, respectively. For the sake of clarity, the Board encourages the IE SA to specify that the complexity and the risks refer to the sector concerned and the data processing activities to which the code applies.

24. With respect to sections from 4.2 to 4.5 of the IE SA's draft accreditation requirements, the Board considers some clarity could be provided with regard to periodic review. This, as well as the meaning of "periodically" and "ad hoc" could be clarified in the explanatory note, in particular by providing examples.

2.2.6 TRANSPARENT COMPLAINT HANDLING

25. With respect to the explanatory note introduced at the beginning of section 5 of the IE SA's draft accreditation requirements ("Transparent Complaint Handling") and its last sentence, the Board is of the opinion that it should be specified what are the 'monitoring body's other monitoring activities'. Therefore, the Board encourages the IE SA to clarify that this term refers to the monitoring activities other than formal decisions.

2.2.7 COMMUNICATING WITH THE IE SA

26. According to the explanatory note provided in section 6 of the IE SA'S draft accreditation requirements, 'a proposed framework for any monitoring body needs to allow for the effective communication *of any actions* carried out by the monitoring body in respect of monitoring of compliance with the Code to the DPC'. In this context, the Board is of the opinion that it should be clarified that not every single action carried out by the monitoring body shall be communicated to the IE SA. The Board underlines that communicating of every single action may create a risk of overloading the IE SA with an excessive amount of information. The same comment applies to section 6.2 and the mention of the "outcome of any audit, review or investigation of a code member's compliance with the code" as well as to section 6.3 and the reference to "procedure for notifying the DPC of any complaints made against it". Therefore, the Board encourages the IE SA to amend the draft accordingly and specify that in general not all the complaints and not every single action, audit, review or investigation vis-à-vis code members is communicated to IE SA.

27. Still with regard to section 6.2 of the IE SA's draft accreditation requirements, the example provided seems to imply that the documentation regarding "any audit, review or investigation of a code member's compliance with the code" or "any review of previously exercised exclusions or suspension from the code" will be made available to the IE SA upon request. However, from the text of the requirement itself, it is unclear whether the notification to the IE SA will take place at the monitoring body's initiative (i.e. irrespective of any request by the SA) or at the request of the IE SA. Therefore, the Board encourages the IE SA to amend the example in order to clarify this issue.

2.2.8 CODE REVIEW MECHANISMS

28. The Board notes that section 7.3 of the draft requirements states that the monitoring body will apply and implement updates, amendments and/or extensions to the Code. Since the updating of the code of conduct is responsibility of the code owner, the Board is of the opinion that, in order to avoid confusion, a reference to the code owner should be made. As an example, section 7.3 of the IE's draft

accreditation requirements could be amended as follows: "The monitoring body shall apply and implement updates, amendments, and/or extensions to the Code, as decided by the code owner". The Board encourages the IE SA to amend the draft accordingly.

2.2.9 LEGAL STATUS

29. As regards section 8 of the IE SA's draft accreditation requirements, the Board notes that in the draft accreditation requirements there is no provision that would explicitly state that the monitoring body must be located within the European Economic Area. The Board is of the opinion that monitoring bodies require an establishment in the EEA. This is to ensure that they can fully uphold data subject rights, deal with complaints and be effectively supervised by the competent SA, so that to guarantee the enforceability of the GDPR. The Board recommends that the IE SA require that the monitoring body has an establishment in the EEA.

30. According to requirement 8.2 of the IE SA's draft accreditation requiements, the monitoring body shall have financial resources to ensure that fines per Article 83(4)(c) GDPR can be imposed on the monitoring body and met. In the Board's opinion, financial capacity shall not prevent small or medium monitoring bodies from being accredited. It is enough to have a legal capability of being fined. Therefore, the Board encourages the IE SA to either delete this requirement or to soften the wording and refer to the monitoring body's responsibilities in general. Moreover, the third paragraph of the example as provided in section 8.3 of the draft requirements should be amended accordingly, and the Board encourages the IE SA to do so.

31. At the same time, 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. Therefore, the Board encourages that the IE SA amend the explanatory note, adding in it a reference to long-term financing.

3 CONCLUSIONS / RECOMMENDATIONS

32. The draft accreditation requirements of the Irish Supervisory Authority create a risk of an inconsistent application of the accreditation of monitoring bodies and the following changes need to be made:

33. As general remarks, the Board recommends that the IE SA:

    1. amend the draft to make a clear distinction between examples and requirements.

34. Regarding 'independence' the Board recommends that the IE SA:

    1. include a reference to the accountability of the monitoring body;
    2. in section 1.2.1 include a reference to the procedures that ensure the functioning of the code of conduct over time;
    3. in section 1.2.5 include obligation on monitoring body to ensure effective monitoring of the services provided by its sub-contractors.

35. Regarding 'legal status' the Board recommends that the IE SA:

    1. require in section 8 that the monitoring body has an establishment in the EEA.

Adopted

4 FINAL REMARKS

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

37. According to Article 64 (7) and (8) GDPR, the IE 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.

38. The IE 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)