Opinion 12/2020 on the draft decision of the competent supervisory authority of Finland 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

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. 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 Finnish Supervisory Authority (hereinafter "FI 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 17 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 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 FI SA to take further action.

8. This opinion does not reflect upon items submitted by the FI 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 FI 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 observes that, according to the general notes of the draft accreditation requirements, the FI SA will review the accreditation of the monitoring body "periodically" according to risk-based approach to ensure that the body still meets the requirements for accreditation. The Board welcomes the provision concerning the periodic re-assessment of the accreditation requirements by the FI SA in order to ensure compliance with the GDPR. However, for the sake of clarity and transparency, the Board encourages the FI SA to provide information on how periodic review will work in practice.

11. With regards to the expertise requirements, section 3.1 of the FI SA's draft accreditation requirements states that the monitoring body shall be compliant with data protection legislation in its own actions. Indeed, it is unclear how the data protection legislation compliance will be checked by the FI SA, for

example, whether a self-declaration of the monitoring body in this regard would be enough or a more comprehensive assessment will be carried out by the SA. Therefore, the Board recommends that the FI SA redraft this requirement in terms of accountability, clarifying that the monitoring body shall demonstrate compliance with data protection legislation.

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

2.2.2 INDEPENDENCE

13. The Board notes that, according to the general notes of the draft accreditation requirements, the requirements shall apply to a monitoring body regardless of whether it is an internal or an external body, unless stated otherwise. The Board is of the opinion that internal monitoring bodies cannot be set up within a code member, but only within a code owner. Therefore, the Board recommends that this is clarified and reflected either in the text of the draft accreditation requirements or as an example.

14. With regard to the first paragraph of the explanatory note under the section 1 of the FI SA's draft accreditation requirements ("Independence"), the Board acknowledges the impartiality of the monitoring body from the code members, the profession, industry or sector to which the code applies. However, the Board is of the opinion that these requirements should be further specified, particularly with regard to any legal and economic links that may exist between the monitoring body and the code owner or code members. For this reason, the Board encourages the FI SA to amend this paragraph accordingly.

15. With regard to the second paragraph of the explanatory note under the "Independence" section of the FI SA's draft accreditation requirements, the Board notes the structural and procedural requirements to ensure independence. The Board recommends that the FI SA redraft the requirements in order to emphasize the fact that it is the monitoring body requesting accreditation that should prove its independence.

16. Furthermore, the Board notes that the monitoring body shall have the financial stability and resources for the operation of its activities and obtain financial support for its monitoring role in a way that does not compromise its independence (section 1.1. and 1.3 of the FI SA's draft accreditation requirements). However, the Board considers that further explanation is needed as to how long-term financial stability of the monitoring body is ensured. In particular, the Board recommends that the FI SA redraft the requirements in order to explain how financial independence is guaranteed in case one or more funding sources are no longer available. Furthermore, the Board considers that section 1.4 of the FI SA's draft accreditation requirements should also include a reference to the need of ensuring clarifications as to how financial independency is ensured with regard to the risks associated with the monitoring body's own activities, for example in case of damages that need to be paid due to the monitoring body's liability. The Board therefore recommends that the FI SA include such reference in the draft accreditation requirements. Finally, the Board considers that section 1.4 of the FI SA's draft accreditation requirements would benefit from the inclusion of some examples with regard to the financial independence of the monitoring body, in order to highlight how the monitoring body can demonstrate that the means by which it obtains financial support would not adversely affect its independence. For instance, the monitoring body would not be considered financially independent if the rules governing its financial support allow a code member, who is under investigation by the

monitoring body, to stop its financial contributions to it, in order to avoid a potential sanction from the monitoring body. The Board encourages the FI SA to provide examples of how the monitoring body can provide such evidence.

17. With regard to the appointment of members/personnel of the monitoring body (section 1.5 of the FI SA's draft accreditation requirements), the Board recommends that the FI SA clarify how the independence of the monitoring body could be demonstrated, aligning the wording of the requirement to this of the Guidelines (see paragraphs 63 to 67), for clarification purposes.

18. Section 1.12 of the FI SA's draft accreditation requirements refers to the organisational structure of the internal monitoring body and ensures its impartiality, by requesting that it has separate members/personnel and management. The Board acknowledges that this wording is based on the Guidelines. Nonetheless, the Board is of the opinion that a strict obligation of using personnel outside the internal monitoring body could be difficult to achieve in certain situations. For this reason, the Board encourages the FI SA to soften the requirement, in order to allow those exceptional situations in which it would not be possible for an internal monitoring body to have separate members/personnel and management from the larger entity it belongs to, as long as there are appropriate safeguards in place to sufficiently mitigate a risk of independence or a conflict of interest (paragraph 66, page 22 of the Guidelines).

19. Section 1.13 of the FI SA's draft accreditation requirements refers to the use of sub-contractors by the monitoring body. The Board is of the opinion that the sub-contractors should be able to ensure the same degree of safeguards provided by the monitoring body in performing their activities, including the same level of competence and expertise. At the same time, the monitoring body should be the ultimate responsible for all the decisions taken related to its monitoring function. Therefore, the Board encourages the FI 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 FI SA to explicitly add this obligation in the draft accreditation requirements.

20. The Board observes that, according to section 1.15 of the FI SA's draft accreditation requirements, when using sub-contractors for processes relating to monitoring actions, the monitoring body shall deliver written contracts or agreements to outline responsibilities etc., as well as documentation of the procedure for subcontracting. The Board encourages the FI 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. Additionally the Board encourages the FI SA to add requirements relating to the risk management of the appointment of the external body.

2.2.3 CONFLICT OF INTEREST

21. The Board takes note of the requirements included in the FI SA's draft 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 explanatory note under section 2 of the draft requirements does not provide enough clarity as to which situations may result in conflict of interest. The Board is of the opinion that, for practical reasons, examples of cases where 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 in the recent years for the code owner, of for any of the organisations adhering to the code in the recent years. Therefore, the Board encourages the FI SA to add some examples, similar to the one provided in this paragraph. Furthermore, the Board encourages the FI SA to redraft the requirement under this section, so that it is clarified that conflicts of interest might also depend on the specificities of the sector(s) to which the CoC applies.

22. The Board acknowledges that the explanatory note under section 2 of the FI SA's draft accreditation requirements refers to the identification of situations likely to create conflict of interest and the fact that measures will be taken in order to avoid such conflict. However, the Board is of the opinion that, with regard to internal monitoring bodies, the requirements relating to the burden of proof of the absence of conflict of interest should be stricter and recommends that the requirements be redrafted accordingly.

23. Section 2.1 of the FI SA's draft accreditation requirements states that the monitoring body shall not provide any services to code members that would adversely affect its impartiality. The Board welcomes this requirement, however it considers that risks to impartiality may arise from a wide range of activities carried out by the monitoring body also vis-à-vis code owners (especially if the monitoring body is internal) or other relevant bodies of the sector concerned. Therefore, the Board encourages the FI SA to supplement the current requirement accordingly.

2.2.4 ESTABLISHED PROCEDURES AND STRUCTURES

24. With regard to established procedures and structures, the Board observes that the requirements under section 4 of the FI SA's draft accreditation requirements are presented in a general manner. The Board is of the opinion that the procedures to monitor compliance with codes of conduct have to be specific enough to ensure a consistent application of the obligations of code monitoring bodies.

25. In particular, such procedures need to address the complete monitoring process, from the preparation of the evaluation to the conclusion of the audit and additional controls to ensure that appropriate actions are taken to remedy infringements and to prevent repeated offences. In addition, the monitoring body should provide evidence of upfront, ad hoc and regular procedures to monitor the compliance of members within a clear timeframe, and check the eligibility of members prior to joining the code.[2] Therefore, the Board recommends that the FI SA develop further these requirements and add examples of the above procedures (such as, procedures providing for audit plans to be carried out over a definite period and on the basis of predetermined criteria, a specific control methodology and the documentation and assessment of the findings as well as the full cooperation by the code members).

26. Section 4.4 of FI SA's the draft accreditation requirements makes reference to descriptions of corrective measures in case of infringement that need to be delivered to the FI SA. The Board is of the opinion that those corrective measures must be determined in the code of conduct, as per article 40(4) GDPR. Therefore, the Board recommends the FI SA to make reference to the list of measures set out

[2] The EDPB provided some examples of such procedures in section 2.2.4 of the Opinion 9/2019 on the Austrian SA draft accreditation requirements for a code of conduct monitoring body pursuant to article 41 GDPR.

in the code of conduct in cases of infringements of the code by a controller or processor adhering to it.

2.2.5 TRANSPARENT COMPLAINT HANDLING

27. Regarding section 5.1 of the FI SA's draft accreditation requirements, the Board acknowledges that the monitoring body should establish effective procedures and structures to handle complaints in an impartial and transparent manner. In this regard, the Board notes that the FI SA's draft accreditation requirements include a description of the procedure for complaints handling. However, the Board is of the opinion that further clarification is needed with regard to the "estimated timeframe" for answering complaints. In this regard, the procedure shall envisage that the monitoring body has to inform the complainant with progress reports or the outcome of the complaint, within a reasonable time frame. 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 requirement is redrafted accordingly.

28. Regarding section 5.4 of the FI SA's draft accreditation requirements, the Boards notes that the monitoring body's decisions, or general information thereof, shall be made publicly available in line with its complaints handling procedure. Without prejudice to national legislation, the Board encourages the FI SA to amend this requirement so that decisions are published when they relate to repeated and/or serious violations, such as the ones that could lead to the suspension or exclusion of the controller or processor concerned from the code, otherwise publication of summaries of decisions or statistical data should be considered adequate. However, data subjects should, in any case, be informed about the status and outcome of their individual complaints, so that the transparency requirements of this procedure are respected.

2.2.6 LEGAL STATUS

With regard to the legal status of the monitoring body, section 8.2 of the FI SA's draft accreditation requirements states that the monitoring body shall have adequate resources for specific duties and responsibilities over a suitable period of 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 monitoring mechanism over time. Thereby, the Board encourages the FI SA to redraft the requirement accordingly.

3 CONCLUSIONS / RECOMMENDATIONS

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

30. Regarding *general remarks* the Board recommends that the FI SA:

1. redraft section 3.1 in terms of accountability, clarifying that the monitoring body shall demonstrate compliance with data protection legislation.

31. Regarding *independence* the Board recommends that the FI SA:

1. clarify, either in the text of the requirements or as an example, that internal monitoring bodies cannot be set up within a code member, but only within a code owner.

2. redraft the second paragraph of the explanatory note, so that is emphasised that it is the monitoring body requesting accreditation the one that should prove its independence.

3. redraft sections 1.1. and 1.6 to explain how financial independence is guaranteed when one or more funding sources are no longer available.

4. include in section 1.4 clarifications as to how financial independence is ensured with regard to the risks associated with the monitoring body's own activities, for example in case of damages that need be paid due to the monitoring body's liability.

5. clarify how the independence of the monitoring body could be demonstrated by aligning the wording of the requirement to this of the Guidelines, with regard to the appointment of members/staff of the monitoring body in section 1.5.

6. add in section 1.13 that, even when subcontractors are used, the monitoring body shall ensure effective monitoring of the services provided by the contracting entity.

32. Regarding *conflict of interest* the Board recommends that the FI SA:

1. redraft the requirements under the explanatory note in section 2 relating to the internal monitoring bodies in a stricter way, in order to include the burden of proof of the absence of conflict of interest.

33. Regarding *established procedures and structures* the Board recommends that the FI SA:

1. further develop under section 4 the procedures to monitor compliance with codes of conduct and includes examples of such procedures.

2. refer in section 4.4 to the list of corrective measures set out in the code of conduct in cases of infringements of the code by a controller or processor adhering to it.

34. Regarding *transparent complaint handling* the Board recommends that the FI SA:

1. redraft section 5.1 to indicate that the procedure for answering complaints shall envisage the obligation for the monitoring body to inform the complainant with progress reports or the outcome of the complaint within a reasonable time frame. Such timeframe can be extended when necessary, taking into account the size of the organisation under investigation, as well as the size of the investigation.

4 FINAL REMARKS

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

36. According to Article 64 (7) and (8) GDPR, the FI 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.

37. The FI 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)