Opinion 19/2020 on the draft decision of the competent supervisory authority of Denmark 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

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 Danish Supervisory Authority (hereinafter "DK 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 27th May 2020.

2 ASSESSMENT

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

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

3. This means that, when drafting the requirements for the accreditation of a body for monitoring codes according to articles 41 (3) and 57 (1) (p) GDPR, all the SAs should cover these basic core requirements foreseen in the Guidelines, and the Board may recommend that the SAs amend their drafts accordingly to ensure consistency.

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

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

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

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

8. Taking into account that:

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

the Board is of the opinion that:

2.2.1 GENERAL REMARKS

9. The Board encourages the DK SA to improve the layout and the format throughout the entire draft accreditation requirements submitted to the Board.

10. In addition, for the sake of clarity, the Board encourages the DK SA to explicitly refer at the first paragraph of the introduction of the draft accreditation requirements to the 01/2019 EDPB Guidelines with regard to the claim that a monitoring body is obligatory in a private sector Codes of Conduct.

11. The Board encourages the DK 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

12. With regard to legal and decision-making procedures of the DK SA draft accreditation requirements (section 1.1), 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 DK SA to amend this paragraph accordingly.

13. Regarding the internal monitoring bodies, the DK SA's draft accreditation requirements provides that the evidence of the monitoring body's independency may be demonstrated by "*a description of the operation of any committees, separate department or personnel that may be involved with the monitoring body*" (section 1.1.5 (h)). However the Board notices that such evidence may not suffice to demonstrate independence, taking into consideration the specific risks for independence that are raised in case of internal monitoring bodies. In view of the above, the Board encourages the DK SA to add more concrete examples of appropriate evidence, such as information barriers, separate reporting structures. The Board is aware of the fact that such examples of evidence are provided in the subsequent section 1.3.5 of the draft accreditation requirements. The Board encourages the DK SA to add such examples at the section 1.1.5 for reasons of clarity and consistency.

14. With regard to the financial independence of DK SA draft accreditation requirements (section 1.2), the Board considers that the financial independence should address the boundary conditions that determine the concrete requirements for financial independence and sufficient resources. Such requirements include the number, size and complexity of the code members (as monitored entities), the nature and scope of their activities (which are the subject of the code) and the risk(s) associated with the processing operation(s). Therefore, the Board encourages the DK SA to redraft the requirements accordingly.

15. With regard to monitoring body's responsibility for its decisions regarding the monitoring activities, the DK SA provided in its draft accreditation requirements (section 1.3.4) "*The personnel of the monitoring body can be held responsible for their activity in accordance with the Danish penal law*". The Board encourages the DK SA to refer in general to the Danish law instead of referring only to the penal law.

2.2.3 CONFLICT OF INTEREST

16. The Board recognizes that one of the biggest risks related to the monitoring body is the risk of impartiality. The Board notes that such 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 DK SA to provide additional clarifications and examples of situations where there is not 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 ESTABLISHED PROCEDURES AND STRUCTURES

17. With regard to the established procedures and structures, the EDPB notes that section 4.1 of the DK SA draft requirements provides that "*Resources should be proportionate to the expected size of code members, as well as the complexity of degree of risk of the relevant data processing and the expected received complaints*". The Board encourages the DK SA, in addition to the "*expected size of the code members*" to add the number of the code members as well for consistency with the section 4.8 of the draft accreditation requirements.

18. Regarding section 4.10 of DK SA's draft accreditation requirements, the Board notes that the monitoring body's decisions, or general information thereof, shall be made publicly available in line with its complaints handing procedure. Without prejudice to national legislation, the Board encourages the DK 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.

2.2.5 COMMUNICATION WITH THE DK SA

19. With respect to the communication with the DK SA (section 6.1), it is stated that "*the monitoring body must set out clear reporting mechanisms to allow for reporting without undue delay of any repeated or serious infringements (which would result in severe actions such as suspensions or exclusion from the code) issued by the monitoring body to the Danish DPA"*. The Board welcomes the fact that not all the complaint and not every single action, audit, review or investigation vis-à-vis code members is communicated to the DK SA, but only the serious cases. However, the Board recommends the DK SA to appropriately add a requirement regarding the reporting of non-serious cases. An example of such requirement could be that the monitoring body should be able to provide relevant information of its action upon DK SA's request.

2.2.6 LEGAL STATUS

20. According to section 8 of the DK SA's draft accreditation requirements "*the monitoring body must demonstrate that it has an appropriate standing to carry out its role under Article 41 (4) of the GDPR and that it is capable of being fined cf. Article 83 (4)(c) of the GDPR and Paragraph 41 (1)(3) of the Danish Data Protection Act ("Databeskyttelsesloven") and when relevant Paragraph 41 (6) of the Danish Data Protection Act*.". The Board is of the opinion that, 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 DK SA to either delete this requirement or to soften the wording and refer to the monitoring body's responsibilities in general and not put an emphasis on the fines.

3 CONCLUSIONS / RECOMMENDATIONS

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

21. Regarding *communication with the DK SA* the Board recommends that the DK SA:
    1. amends section 6.1 so to reflect that not all the cases should be communicated to the DK SA. The Board welcomes the fact that not all the complaint and not every single action, audit, review or investigation vis-à-vis code members is communicated to the DK SA, but only the serious cases. However, the DK SA should add a requirement regarding the reporting of non-serious cases.

4 FINAL REMARKS

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

23. According to Article 64 (7) and (8) GDPR, the DK 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.

24. The DK 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)