Opinion 10/2020 on the draft decision of the competent supervisory authorities of Germany 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 of conduct. 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 German Supervisory Authorities of the Federation and the Länder (hereinafter "DE SAs") have submitted their 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) GDPR, 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's 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's 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 requests 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 DE SAs to take further action.

8. This opinion does not reflect upon items submitted by the DE SAs, 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 DE SAs' draft 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. For the sake of consistency, the Board encourages the DE SAs to use the Guidelines terminology in the draft accreditation requirements and replace the word "criteria" by the word "requirements" in the title of the draft accreditation requirements.

11. The Board notes that in the introductory part under section 3 of the DE SAs' draft accreditation requirements, which defines the powers of the monitoring body, it is stated that the relationship between the monitoring body and the code members is subject to regulation by private law agreement. The Board highlights that the binding nature of the rules of the code of conduct, including those providing for the monitoring mechanism, would result from the (mere) adhesion of the code members to the code, as well as from their membership of the representative association. Whereas contractual arrangements are not, per se, excluded, the Board is of the opinion that the essential elements of the monitoring body's function should be included in the code itself. Additional clauses

may be added in the form of an agreement or contract between the monitoring body and the code member, as long as they do not entail a variation in the essential elements of the monitoring body's function, as set out in the code. Therefore, the Board recommends the DE SAs to specify that the core elements of the monitoring body's function will be included in the code of conduct.

2.2.2 INDEPENDENCE

12. The Board observes that the draft accreditation requirements do not make an explicit reference to "accountability" as one of the four areas in which the monitoring body shall demonstrate independence. The Board considers that the independence of the monitoring body shall be demonstrated in four areas: 1) Legal and decision making procedures, 2) financial, 3) organisational and 4) accountability.[2] Therefore, the Board recommends that the DE SAs include the explicit obligation to demonstrate independence in relation to the accountability of the monitoring body.

13. The Board observes that the introductory paragraph under section 2.2 of the DE SAs' draft accreditation requirements refers to independence of the monitoring body in relation to the "sectoral subject matter of the code of conduct". The Guidelines (paragraph 63) provide further information on how independence of the monitoring body can be demonstrated, for example by demonstrating independence in relation to the profession, industry or sector to which the code applies. Therefore, the Board encourages the DE SAs to redraft this part of the requirements in line with the Guidelines by stating, for example, that the profession, industry or sector to which the code applies are included within the "sectoral subject matter".

14. With regard to section 2.2.1 of the DE SAs' draft accreditation requirements, the Board takes note of all the elements demonstrating the monitoring body's independence with respect to its organisational structure. Among others, it is stated that the monitoring body cannot be penalised for the performance of its tasks. The Board considers that it should be further clarified that the monitoring body assumes responsibility for its activities, and it cannot be penalised by neither the code owner nor the code members. Therefore, the Board encourages the DE SA to redraft this part of the requirement so that the monitoring body is protected against any dismissal or sanction, direct or indirect, for the performance of its duties.

15. The Board notes the requirement for the monitoring body to demonstrate adequate financial resources in order to cover liability claims, among others (section 2.2.2 of the DE SAs' draft accreditation requirements). However, the Board is of the opinion that such a requirement might appear disproportionately burdensome for small and medium enterprises that might be discouraged from applying for accreditation. In this regard, the Board recommends that the DE SAs soften the wording of this section, referring to the monitoring body's responsibilities in a general manner.

2.2.3 CONFLICT OF INTEREST

16. Regarding the individual activities and processes of the monitoring activity that can be outsourced to external service providers (section 2.5 of the DE SAs' draft accreditation requirements), the Board considers that the fact that the obligations applicable to the monitoring body are also applicable to the subcontractors should be clearly stated in the requirements. For this reason, the Board recommends the DE SAs to add the words "and obligations" after the word "requirements" and delete the word "essentially" from the first bullet point under section 2.5.

[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.

2.2.4 ESTABLISHED PROCEDURES AND STRUCTURES

17. Section 2.6.1.2 of the DE SAs' draft accreditation requirements states that the monitoring body will assess whether code members are able to implement the codes of conduct by carrying out a "representative random sampling". According to Article 41 (2)(b) GDPR and paragraphs 70 and 71 of the Guidelines, the monitoring body will need to have appropriate governance structures and procedures, which allow for it to adequately assess the eligibility of controllers and processors to sign up and comply with the code. The Board questions how assessment based on representative random sampling could satisfy the requirements set out in paragraph 71 of the Guidelines, which ask that "*comprehensive vetting procedures"* should be in place in order to "*adequately assess the eligibility of controllers and processors to sign up and comply with the code*". Therefore, the Board recommends that the DE SA deletes reference to "representative random sampling".

18. Section 2.6.1.3 of the DE SAs' draft accreditation requirements, which refers to the verification of the application and monitoring of compliance with the code of conduct, seems reduce the possible monitoring procedures. Depending on the context of the code of conduct, the Board considers that a larger variety of monitoring procedures could also lead to an efficient verification of the application and monitoring of compliance with the code of conduct. For this reason, the Board encourages the DE SAs to redraft this section. For example, references to ad hoc inspections in case of complaints against a particular code member or on site visits to assess compliance with the code could be included, in line with paragraph 72 of the Guidelines.

19. The Board notes that, with regard to the design of the relevant code of conduct, additional tasks may arise for the monitoring bodies of the respective code of conduct (section 2.6.1.5 of the DE SAs' draft accreditation requirements). The Board acknowledges that, but encourages the DE SA to ensure that these additional tasks will not impair the effectiveness and impartiality of the monitoring body's monitoring activities.

2.2.5 TRANSPARENT COMPLAINT HANDLING

20. The Board notes that section 4.2 of the DE SAs' draft accreditation requirements states that publication of the complaints should be carried out both by the monitoring body and the code members. Similar considerations can be made with regards to section 3.1 of the draft accreditation requirements devoted to the code members' obligations to provide the monitoring body with the contact details and contact persons of code members. The Board encourages the DE SAs not to include obligations imposed on code members in the requirements for monitoring bodies and redraft these sections accordingly.

3 CONCLUSIONS / RECOMMENDATIONS

21. The draft accreditation requirements of the German Supervisory Authorities of the Federation and the Länder may lead to an inconsistent application of the accreditation of monitoring bodies and the following changes need to be made:

22. Regarding *general remarks* the Board recommends that the DE SAs:

    1. specify, in section 3, that the core elements of the monitoring body's function will be included in the code of conduct.

23. Regarding *independence* the Board recommends that the DE SAs:

1. include the explicit obligation to demonstrate independence in relation to the accountability of the monitoring body.

2. redraft section 2.2.2 describing the monitoring body's responsibilities in a general manner, with regards to the adequacy of its financial resources.

24. Regarding *conflict of interest* the Board recommends that the DE SAs:

1. add the words "and obligations" after the word "requirements" and deletes the word "essentially" from the first bullet point under section 2.5.

25. Regarding established procedures and structures the Board recommends that the DE SAs:

1. delete the reference to "representative random sampling" from section 2.6.1.2.

4 FINAL REMARKS

26. This opinion is addressed to the German supervisory authorities of the Federation and the Länder and will be made public pursuant to Article 64 (5) (b) GDPR.

27. According to Article 64 (7) and (8) GDPR, the DE SAs shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether they will amend or maintain their draft decision. Within the same period, they shall provide the amended draft decision or where they do not intend to follow the opinion of the Board, they shall provide the relevant grounds for which they do not intend to follow this opinion, in whole or in part.

28. The DE SAs shall communicate the final decision to the Board for inclusion in the register of decisions that 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)