Opinion 14/2022 on the draft decision of the competent supervisory authority of Bulgaria regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR

Adopted on 4 July 2022

Table of contents

1 SUMMARY OF THE FACTS....4
2 ASSESSMENT....4
2.1 General reasoning of the Board regarding the submitted draft accreditation requirements.4
2.2 Analysis of the BG SA's accreditation requirements for Code of Conduct's monitoring bodies 5
2.2.1 GENERAL REMARKS....5
2.2.2 CONFLICT OF INTEREST....7
2.2.3 EXPERTISE....7
2.2.4 ESTABLISHED PROCEDURES AND STRUCTURES....8
2.2.5 TRANSPARENT COMPLAINT HANDLING....8
2.2.6 COMMUNICATION WITH THE BG SA....8
2.2.7 REVIEW MECHANISMS....8
3 CONCLUSIONS / RECOMMENDATIONS....9
4 FINAL REMARKS....9

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 a 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 Bulgarian Supervisory Authority (hereinafter "BG 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 28 March 2022.

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 BG SA to take further action.

7. This opinion does not reflect upon items submitted by the BG 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 BG 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. For the sake of consistency and clarity, the Board encourages the BG SA to replace throughout the draft accreditation requirements the term "Commission for Personal Data Protection" or "CPDP" with the term "Competent Supervisory Authority" in line with the terminology used in the Guidelines. At the same time the Board encourages the BG SA to introduce in the draft requirements a definition of the term «Competent Supervisory Authority», to be understood as the Commission for Personal Data Protection.

10. In general, the Board encourages the BG SA to ensure consistency of the wording throughout the text. For instance in paragraph 4, chapter I, the term "candidate for accreditation" is introduced instead of the accreditation applicant. In paragraph 9, chapter I, section 1; paragraph 13, chapter I, section 3; paragraph 24, chapter II and paragraph 31, chapter IV, the pronouns 'his/her', 'him/her' are used instead of 'its' or 'it' with regards to the accreditation applicant .

11. In addition, the Board encourages the BG SA to complete the text with the missing words where needed (e.g. in section 1, chapter I insert the verb "shall" and in the first sentence of paragraph 12, the verb "must").

12. The Board observes that the last paragraph on page 1 of the introductory chapter and chapter IX (paragraphs 44 to 46) of the BG SA's draft accreditation requirements refer to a monitoring body of a code of conduct as a tool for international transfers. The Board adopted on 22 February 2022 "the Guidelines 04/2021 on Codes of Conduct as tools for transfers". In the opinion of the Board, the Guidelines 04/2021 do not add any additional requirements for the accreditation of monitoring bodies that monitor codes of conduct intended for international transfers. Rather, the Guidelines 04/2021 provide further specifications of the general requirements established by the Guidelines 1/2019 (Section 12) taking into account the specific context of international transfers[2]. Therefore, the Board recommends that the BG SA deletes paragraphs 44 and 46 and add paragraph 45 according to which "the code of conduct serving as a data transfer mechanism may also include additional specific requirements for the monitoring body to be fulfilled at the time of accreditation" in the introductory chapter, along with a general reference to the Guidelines 04/2021.

13. INDEPENDENCE

14. In section 1, chapter I («Legal and decision making procedure») of the BG SA's draft accreditation requirements, the Board encourages the BG SA to clarify the sentence "the nature of the decisions taken" included the examples provided under paragraph 7.

15. As for section 2, chapter I (« Financial independence») of the BG SA's draft accreditation requirements, the Board acknowledges that monitoring bodies should be provided with the financial stability and necessary resources for the effective and independent 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 BG SA replaces "should" by "must" or "shall" and add the word 'independently' in the first sentence of this section which refers to the need for the monitoring body to demonstrate having "sufficient financial resources to carry out effectively the tasks and responsibilities referred to in Article 41(1) of Regulation (EU) 2016/679".

16. With regard to the financial independence (paragraph 10), in the opinion of the Board, 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. Therefore, the Board encourages the BG SA to elaborate further this requirement by providing more examples of how the monitoring body can provide such evidence.

17. With regard to paragraph 11 of section 3 («Legal status and organisational independence»), for the sake of clarity the Board encourages the BG SA to redraft the last part of the second sentence stating that the monitoring body can act as an internal or external monitoring body vis-à-vis the code owner, "with the choice of a particular approach at the discretion of the code owner".

[2] See Section4.2 of the EDPB Guidelines 04/2021 on Codes of Conduct as tools for transfers.

18. Regarding paragraph 12 on internal monitoring bodies, the Board recommends the BG SA to add a requirement to prove that the internal monitoring body has a specific separated budget that is able to manage independently.

19. With regard to paragraph 14 of the BG SA's draft accreditation requirements devoted to the assessment of the structuring of an internal monitoring body, the Board takes note that the second sentence at the end contains the phrase "falling within its scope" and for the sake of clarity, encourages the BG SA to clarify that this sentence, by referring expressly to the scope of the code of conduct.

20. With respect to paragraph 15, addressing the need for the monitoring body to prove, among others, that it has "adequate" human resources for the effective performance its functions under Article 41(1) of Regulation (EU) 2016/679, the Board encourages BG SA to consider making a reference to "sufficient numbers of sufficiently qualified personnel".

21. As regards paragraph 17 of the BG SA's accreditation requirements, the Board understands that, read together with paragraph 19, it establishes that the monitoring body is always the ultimate responsible for the decision-making and for compliance with its obligations, also when it uses subcontractors. The Board encourages the BG SA to clarify the wording as above.

22. In addition, in paragraph 17, the Board recommends that the BG SA adds a clear indication that the monitoring body shall ensure effective monitoring of the services provided by subcontractors.

2.2.2 CONFLICT OF INTEREST

23. With regard to chapter II of the BG SA's draft accreditation requirements, the Board encourages the BG SA to clarify that the phrase "persons employed by it outside its structure" in the first sentence of paragraph 23 includes both natural and legal persons such as subcontractors.

24. As for the second sentence in paragraph 23 which reads "Any interest that results in an advantage of a tangible or intangible nature and/or in the impartial and objective performance of the duties and functions referred to in Article 41(1) of the Regulation is private", the Board notes that the last part of this sentence does not adequately convey the meaning of private interests, as a conflict of interest can be said to arise when it affects the impartial and objective performance of the monitoring body's duties and functions. Therefore, the Board recommends the BG SA to reformulate the sentence as follows "Any interest that results in an advantage of a tangible or intangible nature and/or in affecting the impartial and objective performance of the duties and functions referred to in Article 41(1) of the Regulation is private".

2.2.3 EXPERTISE

25. As regards chapter III, paragraph 26 of the BG SA's draft accreditation requirements, the Board encourages the BG SA to add also a reference to the "knowledge" alongside the "appropriate expertise" in data protection law with respect to the monitoring body's personnel performing decision-making functions.

26. Whilst the BG SA has included all the elements from the Guidelines in these requirements devoted to the expertise of the monitoring body, the Board is of the opinion that the level of the knowledge and expertise in data protection issues should be aligned with the Guidelines. Therefore, the Board encourages the BG SA to align the text with the Guidelines, and require an "in-depth" understanding of data protection legislation.

2.2.4 ESTABLISHED PROCEDURES AND STRUCTURES

27. With regard to paragraph 31, chapter IV, of the BG SA's accreditation requirements («Structures, resources and established procedures for the monitoring of a code of conduct»), the Board encourages the BG SA to clarify that the human resources of the monitoring body must be appropriate to the expected number and size of code members, as well as the complexity or degree of risk of the relevant data processing in line with section 73 of the Guidelines.

2.2.5 TRANSPARENT COMPLAINT HANDLING

28. Regarding paragraph 36, chapter V, of the BG SA's draft accreditation requirements, the Board considers that under section 74 of the Guidelines, the requirements related to the complaint handling process must contain the obligation of the monitoring body to make its decisions or general information thereof, publicly available. Therefore, the Board recommends that the requirement is redrafted accordingly. In addition, the Board encourages the BG SA to clarify that information on the complaint handling process must be publicly accessible.

2.2.6 COMMUNICATION WITH THE BG SA

29. The Board notes that the BG SA's accreditation requirements, chapter VI, provides for annual reporting by the monitoring body to the BG SA. The Board encourages the BG SA to require more regular communication means towards the BG SA during the year in paragraph 40. The Board is of the opinion that the requirements need to address, in particular, such areas as: actions taken in cases of infringement of the code and the reasons for taking them (Article 41 (4) GDPR), periodic reports, reviews or audit findings. The code itself will also outline the communication requirements with the BG SA, including appropriate ad hoc and regular reports. In the case of serious infringements of the code by code members, which result in serious actions such as suspension or exclusion from the code, the BG SA should be informed without undue delay, in line with paragraph 77 of the Guidelines.

2.2.7 REVIEW MECHANISMS

30. The Board observes that, in paragraph 41 of the BG SA's draft accreditation requirements, it is stated that need for change or update of the code of conduct "may arise, for example, in the event of a change in the applicable legislation or in order to take account of the latest technological developments". In line with the Guidelines, the review mechanisms should take also into account any changes in the application and interpretation of the law which have impact upon the data processing carried out by the code members or the provisions of the code. Therefore, the Board encourages the BG SA to appropriately enrich this requirement.

31. With regard to paragraph 42, the Board notes the reference to the review and "ex-post evaluation" of the relevant part of the code. In order to avoid misunderstandings, the Board encourages the BG SA to delete "ex-post".

32. The Board observes that data security obligations may not be included in the scope of a Code of Conduct (e.g. a Code of Conduct may be focused only on transparency toward data subjects). Therefore, the Board encourages the BG SA to add "If applicable" in paragraph 42, second indent, concerning the information on personal data breaches to be provided to the code owner by the monitoring body in the context of the procedure aimed at reviewing periodically the code of conduct.

3 CONCLUSIONS / RECOMMENDATIONS

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

34. Regarding *general remarks* the Board recommends that the BG SA:

1. deletes paragraphs 44 and 46 and add paragraph 45, according to which "The code of conduct serving as a data transfer mechanism may also include additional specific requirements for the monitoring body to be fulfilled at the time of accreditation" in the introductory chapter, along with a general reference to the Guidelines 04/2021.

35. Regarding *independence* the Board recommends that the BG SA:

1. replaces "should" by "must" or "shall" and add the word "independently" in the first sentence of section 2, which refers to the need for the monitoring body to demonstrate having "sufficient financial resources to carry out effectively the tasks and responsibilities of referred to in Article 41(1) of Regulation (EU) 2016/679";

2. Regarding paragraph 12 on internal monitoring bodies, the Board recommends the BG SA to adds a requirement to prove that the internal monitoring body has a specific separated budget;

3. adds in paragraph 17 a clear indication that the monitoring body shall ensure effective monitoring of the services provided by subcontractors.

36. Regarding *conflict of interest* the Board recommends that the BG SA:

1. reformulates the second sentence in paragraph 23 as follows "Any interest that results in an advantage of a tangible or intangible nature and/or in affecting the impartial and objective performance of the duties and functions referred to in Article 41(1) of the Regulation is private".

37. Regarding *transparent complaint handling* the Board recommends that the BG SA:

1. redrafts paragraph 36 to include an obligation for the monitoring body to make its decisions or general information about them publicly available.

4 FINAL REMARKS

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

39. According to Article 64 (7) and (8) GDPR, the BG 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.

40. The BG 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)