Opinion 16/2022 on the draft decision of the competent supervisory authority of Slovenia 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

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 demonstrate how their proposed monitoring body meets the requirements set out in article 41 (2) GDPR to obtain accreditation.

[1] References to the "Union" made throughout this opinion should be understood as references to "EEA".

(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 Slovenian Supervisory Authority (hereinafter "SI 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 SI SA to take further action.

7. This opinion does not reflect upon items submitted by the SI 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 SI 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 notes that on 22 February 2022, "the Guidelines 04/2021 on Codes of Conduct as tools for transfers" were adopted. These guidelines do not add any additional requirements for the accreditation of monitoring bodies that monitor codes of conduct intended for international transfers. Rather, the guidelines 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]. For the sake of clarity, the Board recommends the SI SA to add a reference to the above-mentioned guidelines, which are relevant in the context of monitoring codes of conduct intended for international transfers.

10. For the sake of consistency, the Board encourages the SI SA to adjust the terminology used in the requirements to the one used in the Guidelines, this applies in particular to the following terms. This applies in particular to sections 1.2.1 and 4.2, where it should be referred to the ''expected number and size of the code members, as well as the complexity or degree of risk of the relevant data processing''. In addition, section 4.2 should refer to the need for monitoring bodies to ''actively and effectively monitor compliance'', as well as the need for review procedures to include ''specific incidents''. Moreover, section

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

4.3 should refer to ''annual inspections'' and ''regular reporting''. Finally, the term ''corrective measures'' should be used instead of ''measures'' in sections 4.5 and 5.5.

11. Moreover, 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 in the text of the draft accreditation requirements. In addition, the Board encourages the SI SA to include either in the draft accreditation requirements or in the complementary guidance to the requirements examples of what may constitute an internal monitoring bodies (i.e. ad hoc internal committee or separate department within the organisation of the code owner).

2.2.2 INDEPENDENCE

12. With respect to the definition of independence, the Board encourages the SI SA to elaborate what independence means. To ensure consistency, such clarification could rely on the wording agreed by the Board in the previous opinions, by specifying that the rules and procedures shall allow the monitoring body to perform the monitoring of compliance with a code of conduct in complete autonomy, without being directly or indirectly influenced nor subject to any form of pressure that might affect its decisions.

13. As regards the legal status and decision-making process of the SI SA's draft accreditation requirements (section 1.1), the Board acknowledges the duty of independence of the monitoring body from the code owner and the ''other subjects'' to which the code applies. In this regard, the Board encourages the SI SA to clarify which are the ''other subjects'' that might influence the decisions of the monitoring bodies by referring to ''the code members, the profession, industry or sector to which the code applies and the code owner itself'' (Paragraph 63 of the Guidelines).

14. With regard to the same section, last sentence, the Board encourages the SI SA to clarify that the requirement to demonstrate the implementation of complementary measures applies to ''internal monitory bodies'', which shall ensure that the independence of their ''monitoring activities'' is not at stake. Furthermore, the Board encourages the SI SA to amend this section to reflect the requirement, as provided in paragraph 65 of the Guidelines, that the internal monitoring body has separate staff and management from other areas of the organisation.

15. Moreover, as the section 1.1.4 refers to the terms "undue" influence, the Board encourages the SI SA to delete the word "undue" considering that a monitoring body must be free not only from "undue" but from any external influence.

16. Further, in section 1.2.2, a reference not only to financial resources but also to other resources should be mentioned. Therefore, the Board recommends that the SI SA require that the monitoring body should have access to adequate financial and ''other resources'' to fulfil its monitoring responsibilities.

17. Finally, with respect to internal monitoring bodies (section 1.2.4), the Board recommends the SI SA to add a requirement to prove that the internal monitoring body has a specific separated budget that is able to manage independently.

18. With regard to section 1.3 of the draft requirements, the Board observes that the reference to organisational independence of the monitoring body is not entirely complete. In particular, the Board notes that the monitoring bodies should be composed of an adequate number of personnel so that they are able to fully carry out the monitoring functions, reflecting the sector concerned and the risks of the processing activities addressed by the code of conduct. Personnel of the monitoring body shall be responsible and shall retain authority for their decisions regarding the monitoring activities. These organisational aspects could be demonstrated not only through the procedure to appoint the monitoring

body personnel, the remuneration of the said personnel, the duration of the personnel's mandate, but also through contract or other formal agreement with the monitoring body. Therefore, the Board recommends that the SI SA provide the above-mentioned references regarding the independence of the monitoring body in performing its tasks and exercising its powers, in accordance with the Guidelines.

19. In addition, the Board encourages the SI SA to, in line with what is mentioned under paragraph 14 of this Opinion, amend the requirement in section 1.3.4 in order to reflect the need for internal monitoring bodies to have separate staff and management.

2.2.3 CONFLICT OF INTEREST

20. As a general remark in this section, the Board is of the opinion that, for practical reasons, more detailed guidance as to in which situations a 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 for the code owner, or for any of the organisations adhering to the code. Therefore, the Board encourages the SI SA to add some guidance, similar to the one provided in this paragraph.

21. Moreover, the Board encourages the SI SA to clarify in section 2.3 that the staff chosen by the monitoring body or other body should be ''independent of the code member''.

2.2.4 EXPERTISE

22. With regard to section 3.1, the Board acknowledges the requirement for the monitoring body to demonstrate that it has expertise in relation to the specific data processing activities addressed by the code. However, as agreed by the Board in the previous opinions, other factors such as the size of the sector concerned, the different interests involved and the risks of these processing activities should be taken into account. The Board therefore recommends that this is clarified in the draft accreditation requirements.

23. Moreover, the Board notes that SI SA's expertise requirements do not differentiate between staff at the management level and, therefore, in charge of the decision-making process, and staff at the operating level, conducting the monitoring activities. In this regard, the Board encourages the SI SA to clarify in section 3.2 which requirement should be met by the staff performing the monitoring function and the personnel making the decisions.

2.2.5 ESTABLISHED PROCEDURES AND STRUCTURES

24. Regarding section 4.1, the Board notes that when new members join the code, the monitoring body should, in any case, have a procedure in place to verify that the processing of personal data by these members falls within the scope of the code in question. Therefore, the Board encourages the SI SA not to formulate this provision as an example.

2.2.6 TRANSPARENT COMPLAINT HANDLING

25. The Board observes that section 5.5 of the SI SA's draft accreditation refers to the obligation of the monitoring body to inform the SA of the measures taken and the reasons for taking them. In line with paragraph 77 of the Guidelines, the Board recommends that the SI SA clarify that this communication should be made ''without undue delay'', and provide that this notification should be made to '' the code member, the code owner, the competent SA and, where required, all concerned SAs''.

26. Regarding section 5.8 of the SI SA's draft accreditation requirements, the Board notes that the monitoring body shall, on a regular basis, publish statistical data with the results of the monitoring activities. Without

prejudice to national legislation, the Board encourages the SI 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.

2.2.7 COMMUNICATION WITH THE SI SA

27. The Board understands that section 6.1 of the requirements refers to the information that the monitoring body will provide to the SI SA upon request. The Board is of the opinion that the requirement to communicate ''any actions'' need to address 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. Therefore, the Board encourages the SI SA to clarify this requirement accordingly.

28. In addition, the Board recommends that the SI SA clarify the notion of ''substantial changes'' in section 6.2. In particular, it should be specified that substantial changes include but are not limited to any changes that impacts the ability of the monitoring body to perform its tasks in an independent, impartial and efficient manner. In addition, it should be clarified that not only the above-mentioned changes but also the one listed in section 6.3 are to be communicated to the SI SA without undue delay. Finally, the Board encourages the SI SA to clarify in its draft accreditation requirements the notion of "any changes to the basis of accreditation" referred to in subsection 6.3, point c.

2.2.8 REVIEW MECHANISMS

29. The draft accreditation requirements (section 7.1, second sentence) refer to the possibility for any other entity referred to in the code to be granted an active and participative role in the code review process. The Board notes it is the role of the code owner to ensure the continued relevance and compliance of the code of conduct with applicable legislation. Whilst the monitoring body is not responsible to carry out that task, it shall contribute to any review of the code. The Board therefore encourages the SI SA to specify that the monitoring body shall apply and implement these updates, amendments, and/or extensions to the Code on behalf of the code owner.

30. In addition, the Board encourages the SI SA to specify in section 7.4 that the annual report prepared by the monitoring body should include reviews and/or changes made to the code.

2.2.9 SUBCONTRACTORS

31. In relation to section 9.3, the Board encourages the SI SA to better clarify that notwithstanding the sub-contractor's responsibility and obligations, the monitoring body is always the ultimate responsible for the decision-making and for compliance.

32. Furthermore, the Board recommends that the SI SA clarify the notion of ''substantial changes'' in section 9.2., in line with what is mentioned under paragraph 28 of this Opinion.

3 CONCLUSIONS / RECOMMENDATIONS

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

10. Regarding *general remarks* the Board recommends that the SI SA:

- to add a reference to the Guidelines 04/2021, which are relevant in the context of monitoring codes of conduct intended for international transfers.
- clarify in the text of the requirements that internal monitoring bodies cannot be set up within a code member, but only within a code owner.

11. Regarding *independence* the Board recommends that the SI SA:

- provide in section 1.1.4 the requirement for monitoring bodies to have access to adequate financial and ''other resources'' to fulfil their monitoring responsibilities.
- add in section 1.2.4 a requirement to prove that the internal monitoring body has a specific separated budget that is able to manage independently.
- include in section 1.3 the references mentioned in paragraph 18 of this Opinion concerning the independence of the monitoring body in performing its tasks and exercising its powers.

12. Regarding *expertise* the Board recommends that the SI SA:

- clarify that other factors such as the size of the sector concerned, the different interests involved and the risks of these processing activities should be taken into account in order to assess the level of expertise of the monitoring body.

13. Regarding *transparent complaint handling* the Board recommends that the SI SA:

- clarify that the obligation of the monitoring body to communicate the measures taken and the reasons for taking them should take place ''without undue delay'', and provide that this notification should be made not only to the SA but also to ''the code member, the code owner, the competent SA and all concerned SAs''.

14. Regarding *communication with the SI SA* the Board recommends that the SI SA:

- clarify in section 6.2 that substantial changes include but are not limited to any changes that impacts the ability of the monitoring body to perform its tasks in an independent, impartial and efficient manner, and specify that the changes listed in section 6.3 are to be communicated to the SI SA without undue delay.

15. Regarding *legal status* the Board recommends that the SI SA:

- clarify the notion of ''substantial changes'' in section 9.2 in line with what is mentioned under paragraph 28 of this Opinion.

4 FINAL REMARKS

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

17. According to Article 64 (7) and (8) GDPR, the SI 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.

18. The SI 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)