Opinion 13/2020 on the the draft decision of the competent supervisory authority of Italy 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, as last modified and adopted on 10 September 2019

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 Italian Supervisory Authority (hereinafter "IT 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 13 February 2019.

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 IT SA to take further action.

8. This opinion does not reflect upon items submitted by the IT 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 IT 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 and clarity, the EDPB encourages the IT SA to replace throughout the draft accreditation requirements the terms "association/ organisation owning the CoC" and "association/ organisation submitting the CoC" with the term "Code owner" in line with the terminology used in the Guidelines.

2.2.2 INDEPENDENCE

11. The Board observes that, in section 3 of the IT SA's draft accreditation requirements ("autonomy, independence, impartiality"), it is mentioned that "*accreditation shall be granted if autonomy, independence and impartiality of the monitoring body as required to fulfil the respective monitoring*

obligations are demonstrated (...)". The Board encourages the IT SA to delete reference to autonomy, for the sake of clarity and consistency.

12. For the sake of clarity, the Board encourages the IT SA to clarify the meaning of "membership of the monitoring body" and "term of the monitoring body" under section 3a ("legal status and decision-making process"), first paragraph of the draft accreditation requirements

13. Furthermore, 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 the second paragraph of section 3a.

14. With regard to the legal status and decision-making process of the IT SA's draft accreditation requirements (section 3a), 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 IT SA to amend this paragraph accordingly.

15. With regard to the financial independence of the IT SA's draft accreditation requirements (section 3b), the Board notes that the monitoring body shall obtain financial support for its monitoring role in a way that does not compromise its independence. 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 IT SA amend the requirements in order to explain how financial independence is guaranteed in case one or more funding sources are no longer available.

16. Furthermore, the Board considers that the section concerning the financial independence should address the boundary conditions that determine the concrete requirements for financial independence and sufficient resources. These 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 IT SA to redraft the requirements accordingly.

17. The Board takes note of the requirements with regard to the organisational independence, under section 3c of the draft accreditation requirements, however it considers that these requirements should be further specified. For this reason, the Board encourages the IT SA to redraft this part of the requirements by adding examples of how such independence can be achieved. For example, the organisational independence can be demonstrated with a differentiated payroll, analytical accounting systems with different responsibility centres or any other logical separation that can rise firewalls between the monitoring body and the code owners or code members.

18. The second explanatory note under section 3c of the IT SA's draft accreditation requirements ("organisational independence") 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 IT 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 IT SA to explicitly add this obligation in the draft accreditation requirements.

2.2.3 CONFLICT OF INTEREST

19. The Board takes note of all the requirements included in the IT 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 (section 4). The Board encourages the IT SA to add examples in the requirements in this respect. For example, employees of the monitoring body should be required to report possible conflicts of interest.

20. Furthermore, the Board is of the opinion that, for practical reasons, examples of cases where 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 IT SA to add some examples, similar to the one provided in this paragraph.

3 CONCLUSIONS / RECOMMENDATIONS

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

22. Regarding *independence* the Board recommends that the IT SA:

1. clarify in the second paragraph of section 3a that internal monitoring bodies cannot be set up within a code member, but only within a code owner.

2. explain in section 3b how financial independence is guaranteed in case one or more funding sources are no longer available.

3. add in section 3c that even when subcontractors are used, the monitoring body shall ensure effective monitoring of the services provided by the contracting entity.

4 FINAL REMARKS

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

24. According to Article 64 (7) and (8) GDPR, the IT 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.

25. The IT 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)