Opinion 37/2021 on the draft decision of the competent supervisory authority of Malta regarding the approval of the requirements for accreditation of a code of conduct monitoring body pursuant to article 41 GDPR

Adopted on 30 November 2021

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 MT SA's accreditation requirements for Code of Conduct's monitoring bodies 5

2.2.1 GENERAL REMARKS 5

2.2.2 LEGAL STATUS 6

2.2.3 INDEPENDENCE 7

2.2.4 CONFLICT OF INTEREST 8

2.2.5 EXPERTISE 9

2.2.6 ESTABLISHED PROCEDURES AND STRUCTURES 9

2.2.7 TRANSPARENT COMPLAINTS HANDLING 9

2.2.8 COMMUNICATION WITH THE COMPETENT SUPERVISORY AUTHORITY 10

2.2.9 CODE REVIEW MECHANISM 10

2.2.10 REVOCATION OF A MONITORING BODY 10

3 CONCLUSIONS / RECOMMENDATIONS 10

4 FINAL REMARKS 11

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 Office of the Information and Data Protection Commissioner of Malta (hereinafter "MT 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 5 October 2021.

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 MT SA to take further action.

7. This opinion does not reflect upon items submitted by the MT 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 MT 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. One of the tasks of the Board is to ensure consistency between requirements submitted by national supervisory authorities. For the sake of clarity the Board considers that the overall structure of the draft requirement submitted by MT SA should be improved. Therefore, with the aim to facilitate the assessment and ensure consistency, the Board encourages MT SA to follow the structure of the Guidelines in the draft requirements and to adjust titles of the subsection and their order to it.

10. For the sake of consistency, the Board encourages MT SA to adjust terminology used in the requirements to the terminology used in the Guidelines, this applies in particular to the following terms: 'code owners', "monitoring body", 'accreditation'. Also, clarification of what is meant by "legal position" (section 3.2), "good repute", "suitability in decision-making", "beneficial owners" (section 4.1.vii), analytical accounting systems (section 4.3.ii), any logical separation raising barriers between

the monitoring body and the code owners / members (section 4.3.iii) other relevant bodies (section 5), principle of natural justice (section 7) and substantial change (section 9) would be of help. Moreover, as throughout the text MT SA is using the term "undue" influence, the Board suggests to delete the word "undue" as a monitoring body must be free not only from "undue" but from any external influence.

11. The Board encourages MT SA to correct several typos in the opinion, such as non-for-profit in section 3.1. In the same section, the Board encourages MT SA, for the sake of consistency, to state that a monitoring body must be "established" (not "incorporated") in the European Union.

12. The Board is of the opinion that examples help in understanding the draft requirements. Therefore, the Board encourages MT SA to include in the draft accreditation requirements some additional examples. In particular, the Board invites MT SA to add:

- example of what is meant by "good repute" (section 3.2);
- examples of additional duties that may be performed by the monitoring body (section 3.5);
- examples of monitoring body's services to code members which could adversely affect its independence (section 4.1);
- examples regarding how to ensure the independence of the monitoring body in performing its tasks and exercising its powers (section 4.3);
- examples of situations where there is a conflict of interests and where there is no such conflict (section 5);
- examples of how the monitoring body may demonstrate expertise (section 6);
- examples of sanctions that may be set out in the code of conduct (section 8);
- examples of substantial changes that may affect the capacity of the monitoring body to monitor the code (section 9).

13. For the sake of consistency, with respect to the application of the code, the Board encourages MT SA to move section 3.4 to the "Introduction" part of the requirements, since it seems to connect to all requirements and not just the legal status requirement. Moreover, the Board encourages MT SA to further expand the section on application procedure. In particular, this section could state for example, that accreditation as a monitoring body is only possible in relation to the subject matter of one or more specific codes of conduct pursuant to Article 41 (1) of the GDPR, contain minimum requirements for the application for an accreditation and state in which form applications for accreditation must be submitted.

2.2.2 LEGAL STATUS

14. As regards the provision stating that in the event that the monitoring body is established in an EEA country other than Malta, the legal framework of such EEA country shall incorporate legal provisions that are substantially equal to Maltese legislation regulating legal and natural persons, in particular with regards to their liability at law, the Board encourages MT SA to clarify the meaning of this provision, in particular the term "substantially equal".

15. In the same section in the sentence, “[t]he requirements indicated herein shall apply to both external and internal proposed monitoring bodies, unless specified otherwise” the Board encourages MT SA to clarify what it means by “unless specified otherwise”.

16. In section 3.2, the Board is of the opinion that it should be explicitly mentioned that the monitoring body should have a legal capability of being fined. In the same section, the Board encourages the MT SA to strengthen the wording when referring to evidence by stating that it “shall” not “may” include evidences as listed by MT SA.

17. In section 3.3, the Board encourages the MT SA to state that the monitoring body “have access” instead of “shall have access” to necessary resources.

18. With respect to section 3.5 “Other functions”, the Board encourages MT SA to move it to the “Independence” section instead, as this provision relates more to the independent functioning of the monitoring body rather than its legal status.

19. In section 3.6 of the draft requirements, MT SA correctly states that the monitoring body may farm out certain monitoring activities to other entities acting as sub-contractors. In the opinion of the Board, to a limited extent and under certain conditions it is possible for the monitoring body to outsource certain activities. However, it should be clear that the decision-making process cannot be outsourced. Therefore, the Board encourages MT SA to clarify in the requirements whether "certain monitoring activities" refer to the decision-making.

20. As regards section 3.6 the Board considers that the monitoring body, in addition to be the ultimate responsible for the decision-making, is also responsible for compliance when it uses subcontractors. The Board encourages MT SA to add a relevant reference. Moreover, the Board encourages MT SA to include an explicit requirement for subcontractors to comply with their data protection obligations.

21. Additionally, the Board underlines the need to specify requirements relating to the termination of the contract, in particular so as to ensure that the subcontractors fulfil their data protection obligations related to such a termination, and encourages the MT SA to add such remark.

22. As regards the same section, the Board is of the opinion that the code of conduct itself needs to demonstrate that the operation of the code’s monitoring mechanism is sustainable over time and covering worst-case scenarios, such as the monitoring body being unable to perform the monitoring function. In this regard, a monitoring body should demonstrate that it can deliver the code of conduct’s monitoring mechanism over a suitable period of time. Therefore, the Board recommends the MT SA to explicitly require that monitoring bodies demonstrate continuity of the monitoring function over time. Moreover, a clear indication that financial stability and resources need to be accompanied with the necessary procedures to ensure the functioning of the code of conduct over time should be added.

23. For the sake of consistency, the Board encourages MT SA to replace term “responsibilities at law” with “ultimate responsibility”, as the monitoring body has responsibility not only according to law, but the ultimate responsibility for decision-making and compliance when it uses subcontractors.

2.2.3 INDEPENDENCE

24. With respect to independence, the Board believes that it should be ensured at any time, not only during the decision-making process, therefore in section 4 of MT SA’s draft requirements, the Board recommends the MT SA to add the following wording “These rules and procedures shall therefore

ensure the complete autonomy of the monitoring body from any direct or indirect influence or pressure at any time".

25. As regards legal and decision-making procedures and ensuring that the decision-making personnel of the monitoring body has no convergent interests with the entities subject to monitoring, the Board is of the opinion that the monitoring body must (and not "may") bring information concerning the activities (gainful or not) in which its personnel is engaged (section 4.1.vi) to the code owner, thus encourages MT SA to incorporate relevant clarification in its requirements.

26. As regards section 4.1.viii, the Board underlines that the duration or expiration of the mandate of the monitoring body must be regulated in such a way to prevent overdependence on a renewal or fear of losing the appointment, to an extent that adversely affects the independence in carrying out the monitoring activities by the monitoring body. The Board encourages the MT SA to explicitly mention this matter in its requirements and to provide examples regarding duration and expiration.

27. With respect to section 4.1 and requirements an internal body has to demonstrate, the Board notes that not all requirements from point 65 of Guidelines were mentioned by MT SA. The Board encourages the MT SA to add missing requirements.

28. In the section 4.2 "Financial independence" a reference not only to financial resources but also to other resources should be mentioned, thus the Board recommends that the MT SA require that the monitoring body should have access to adequate financial and other resources to fulfil its monitoring responsibilities, especially for the accreditation of a natural person.

29. Regarding section 4.2 on the financial independence of the monitoring body, the Board notes that the elements to be taken into account in this assessment, have not been addressed. Such elements include the size and complexity of the code members (as monitored entities), the nature and scope of their activities (as the subject of the code) and the risk(s) associated with the processing operation(s). Therefore, the Board encourages MT SA to add these elements to the relevant section of the requirements.

30. The monitoring body shall have an adequate and proportionate number of staff members. These aspects could be demonstrated through the procedure to appoint the monitoring body personnel, the remuneration of the said personnel, as well as the duration of the personnel's mandate, contract or other formal agreement with the monitoring body. Therefore, the Board recommends to MT SA to provide suitable requirements for organisational aspects of the independence of the monitoring body and add the above-mentioned references regarding the independence of the monitoring body in performing its tasks and exercising its powers, in accordance with the Guidelines.

31. Finally, with respect to internal monitoring bodies, the Board encourages the MT SA to add a requirement to prove that a specific, separated budget is allocated to such bodies by the code owner.

2.2.4 CONFLICT OF INTEREST

32. With respect to section 5 of the requirements, and the provision stating that "the monitoring body must remain free from external or internal influence" the Board encourages the MT SA to clarify what is meant by "internal influence" or use the term "direct or indirect" influence. In this context, it should be underlined that the Guidelines in paragraph 68 only refer to "free from external influence, whether

direct or indirect, and shall neither seek nor take instructions from any person, organisation or association."

33. As regards Section 5 and the sentence "A monitoring body which is internal must be appropriately protected from any sort of sanctions or interference (whether direct or indirect) by the code owner, other relevant bodies, or code members as a consequence of the fulfilment of its tasks", the Board encourages the MT SA to delete the reference to "internal", as this requirement shall apply also to external monitoring bodies.

2.2.5 EXPERTISE

34. The Board observes that in the section 6 of the draft requirements the MT SA makes distinction between legal and technical personnel. The Board encourages the MT SA to clarify that the technical requirements of the personnel will depend on whether this is necessary for the code at stake or not.

35. Moreover, the Board recommends to clarify in this section that in order to demonstrate expertise of the staff on specific personal data processing, different interests involved and the risks of the processing activities addressed by the code should also be taken into account.

2.2.6 ESTABLISHED PROCEDURES AND STRUCTURES

36. In section 7 of the draft requirements, MT SA stated that "The monitoring body shall remain responsible to ensure that any information entered into its possession whilst carrying out its monitoring functions remains confidential unless it is required to disclose such information or it is exempt by law". The Board encourages the MT SA to clarify what it meant by situations requiring disclosure of information, different from exemption by law.

37. As regards section 7.2 "Monitoring of compliance", the monitoring body must demonstrate that it has a procedure for the investigation, identification and management of code member infringements to the code and additional controls to ensure that appropriate action is taken to remedy such infringements of the code. The Board encourages the MT SA to include relevant reference in the requirements. Moreover, as there are also other ways than audit to monitor controllers' and processors' compliance with the code the Board encourages MT SA to make clear that review procedures can include not only audits, but also inspections, reporting and the use of self-monitoring reports or questionnaires.

38. The Board encourages MT SA to avoid using the term "penalties" and use "corrective measures" instead.

2.2.7 TRANSPARENT COMPLAINTS HANDLING

39. In Section 8 "Transparent Complaints Handling", MT SA mentioned that handling complaints "is organized in a manner that a dedicated and segregated section of the monitoring body oversees complaints, when feasible". The Board encourages MT SA to explain in which cases oversight by a dedicated and segregated section would not be possible. Moreover, the Board suggests adding a requirement that where it is not possible to have such a separated section, a justification should be brought forward.

Adopted

40. With respect to the same section, the Board encourages MT SA to add provisions regarding publication of the decisions - at least regarding publication of summaries or statistical data. Moreover, the Board encourages MT SA to add procedural requirements regarding complaint-handling process, in particular the right to be heard and duty to provide relevant information.

2.2.8 COMMUNICATION WITH THE COMPETENT SUPERVISORY AUTHORITY

41. As regards section 9 “Communication with the competent supervisory authority”, for the sake of consistency with other opinions, the Board encourages MT SA to replace the reference to “communication channels” with “reporting mechanism”.

2.2.9 CODE REVIEW MECHANISM

42. As regards section 10 “Code review mechanism”, the Board encourages MT SA to align the wording of this section with the wording of the Guidelines, and explicitly mention that the review mechanisms should take into account any changes in the application and interpretation of the law or where there are new technological developments which have impact upon the data processing carried out by the code members or the provisions of the code.

43. In the same section, the Board encourages MT SA to ensure that not only the monitoring body but also any other entity referred to in the code of conduct may, if appropriate, be granted an active and participative role in the code review process.

2.2.10 REVOCATION OF A MONITORING BODY

44. In section 11 “Revocation of a monitoring body” in the sentence “In such a case, depending on the circumstances, prior to the revocation, the competent supervisory authority may give the monitoring body the opportunity to urgently address the issues encountered and remediate to its infringements by taking the necessary corrective actions.” The Board encourages MT SA to replace “may” with “should”. In order to align the wording of the draft requirements with paragraph 87 of the Guidelines, in the sentence “[i]n the case of transnational codes, the competent supervisory authority should consult and seek the views of the CSAs and communicate that it intends to revoke the accreditation of the monitoring body to all CSAs and to the Board” the Board encourages MT SA to replace word “CSAs” with “concerned Supervisory Authorities”.

3 CONCLUSIONS / RECOMMENDATIONS

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

46. Regarding ”legal status”the Board recommends that MT SA:

- explicitly require that monitoring bodies must demonstrate continuity of the monitoring function over time;

47. Regarding ”independence” the Board recommends that MT SA:

- add a reference to the fact that independence is ensured at any time, not only during the decision-making process;
- require that the monitoring body should have access not only to financial but also other resources necessary to fulfil its monitoring responsibilities;
- provide suitable requirements for organisational aspects of the independence of the monitoring body;

48. Regarding ”expertise” the Board recommends that MT SA:

- clarify that in order to demonstrate expertise of the staff on specific personal data processing, different interests involved and the risks of the processing activities addressed by the code should be taken into account.

4 FINAL REMARKS

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

50. According to Article 64 (7) and (8) GDPR, the MT 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.

51. The MT 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)