Opinion 4/2023 on the draft decision of the competent supervisory authority of Malta regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)

Adopted on 3 February 2023

Table of contents

The European Data Protection Board

Having regard to Article 63, Article 64 (1c), (3) - (8) and Article 43 (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 (hereafter "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 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (hereafter GDPR) throughout the European Economic Area. In compliance with Article 64.1 GDPR, the Board shall issue an opinion where a supervisory authority (SA) intends to approve the requirements for the accreditation of certification bodies pursuant to Article 43. The aim of this opinion is therefore to create a harmonised approach with regard to the requirements that a data protection supervisory authority or the National Accreditation Body will apply for the accreditation of a certification body. Even though the GDPR does not impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by encouraging SAs to draft their requirements for accreditation following the structure set out in the Annex to the EDPB Guidelines on accreditation of certification bodies, and, secondly by analysing them using a template provided by EDPB allowing the benchmarking of the requirements (guided by ISO 17065 and the EDPB guidelines on accreditation of certification bodies).

(2) With reference to Article 43 GDPR, the competent supervisory authorities shall adopt accreditation requirements. They shall, however, apply the consistency mechanism in order to allow generation of trust in the certification mechanism, in particular by setting a high level of requirements.

(3) While requirements for accreditation are subject to the consistency mechanism, this does not mean that the requirements should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB opinion is not to reach a single EU set of requirements but rather to avoid significant inconsistencies that may affect, for instance trust in the independence or expertise of accredited certification bodies.

(4) The "Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)" (hereinafter the "Guidelines"), and "Guidelines 1/2018 on certification and identifying certification criteria in accordance with article 42 and 43 of the Regulation 2016/679" will serve as a guiding thread in the context of the consistency mechanism.

(5) If a Member State stipulates that the certification bodies are to be accredited by the supervisory authority, the supervisory authority should establish accreditation requirements including, but not

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

limited to, the requirements detailed in Article 43(2). In comparison to the obligations relating to the accreditation of certification bodies by national accreditation bodies, Article 43 provides fewer details about the requirements for accreditation when the supervisory authority conducts the accreditation itself. In the interests of contributing to a harmonised approach to accreditation, the accreditation requirements used by the supervisory authority should be guided by ISO/IEC 17065 and should be complemented by the additional requirements a supervisory authority establishes pursuant to Article 43(1)(b). The EDPB notes that Article 43(2)(a)-(e) reflect and specify requirements of ISO/IEC 17065 which will contribute to consistency.[2]

(6) The opinion of the EDPB shall be adopted pursuant to Article 64 (1)(c), (3) & (8) 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 OPINION:

1 SUMMARY OF THE FACTS

1. The Office of the Information and Data Protection Commissioner (hereinafter "MT SA") has submitted its draft accreditation requirements under Art. 43 (1)(b) GDPR to the EDPB. The file was deemed complete on 27 October 2022. The National Accreditation Board (Malta), as national accreditation body (NAB), will perform accreditation of certification bodies to certify the use of GDPR certification criteria. This means that the NAB will use ISO/IEC 17065 and the additional requirements set out by the MT SA, once they are approved by the MT SA, following an opinion from the Board on the draft requirements, to accredit certification bodies.

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 EDPB regarding the submitted draft decision

3. The purpose of this opinion is to assess the accreditation requirements developed by a SA, either in relation to ISO 17065 or a full set of requirements, for the purposes of allowing a national accreditation body or a SA, as per Art. 43(1) GDPR, to accredit a certification body responsible for issuing and renewing certification in accordance with Art. 42 GDPR. This is without prejudice to the tasks and powers of the competent SA. In this specific case, the Board notes that the Maltese national law prescribes that its NAB is responsible for the issuance of accreditation. The MT SA has therefore drafted additional requirements in accordance with the Guidelines, which should be used by its NAB

[2] Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation, para. 39. Available at: https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_en

when issuing accreditation. To this end, the MT SA has developed a set of requirements specifically for accreditation of certification bodies in conjunction with a set of certification criteria that is yet to be formally approved.

4. This assessment of MT SA's additional accreditation requirements is aimed at examining on variations (additions or deletions) from the Guidelines and notably their Annex 1. Furthermore, the EDPB's Opinion is also focused on all aspects that may impact on a consistent approach regarding the accreditation of certification bodies.

5. It should be noted that the aim of the Guidelines on accreditation of certification bodies is to assist the SAs while defining their accreditation requirements. The Guidelines' Annex does not constitute accreditation requirements as such. Therefore, the accreditation requirements for certification bodies need to be defined by the SA in a way that enables their practical and consistent application as required by the SA's context.

6. The Board acknowledges the fact that, given their expertise, freedom of manoeuvre should be given to NABs when defining certain specific provisions within the applicable accreditation requirements. However, the Board considers it necessary to stress that, where any additional requirements are established, they should be defined in a way that enables their practical, consistent application and review as required.

7. The Board notes that ISO standards, in particular ISO/IEC 17065, are subject to intellectual property rights, and will therefore not refer to the text of the related document in this Opinion. As a result, the Board decided to, where relevant, point towards specific sections of the ISO Standard, without, however, reproducing the text.

8. Finally, the Board has conducted its assessment in line with the structure foreseen in Annex 1 to the Guidelines (hereinafter "Annex"). Where this Opinion remains silent on a specific section of the MT SA's draft accreditation requirements, it should be read as the Board not having any comments and not asking the MT SA to take further action.

9. This Opinion does not reflect upon items submitted by the MT SA, which are outside the scope of Art. 43 (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 Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently:

a. addressing all the key areas as highlighted in the Guidelines Annex and considering any deviation from the Annex.

b. independence of the certification body

c. conflicts of interests of the certification body

d. expertise of the certification body

e. appropriate safeguards to ensure GDPR certification criteria is appropriately applied by the certification body

f. procedures for issuing, periodic review and withdrawal of GDPR certification; and

g. transparent handling of complaints about infringements of the certification.

10. Taking into account that:

a. Article 43 (2) GDPR provides a list of accreditation areas that a certification body need to address in order to be accredited;

b. Article 43 (3) GDPR provides that the requirements for accreditation of certification bodies shall be approved by the competent Supervisory Authority;

c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for certification bodies and may decide to conduct the accreditation of certification bodies itself;

d. Article 64 (1) (c) GDPR provides that the Board shall issue an opinion where a supervisory authority intends to approve the accreditation requirements for a certification body pursuant to Article 43(3);

e. If accreditation is carried out by the national accreditation body in accordance with ISO/IEC 17065/2012, the additional requirements established by the competent supervisory authority must also be applied;

f. Annex 1 of the Guidelines on Accreditation of Certification foresees suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a certification body by the National Accreditation Body;

the Board is of the opinion that:

2.2.1 PREFIX

11. The Board acknowledges the fact that terms of cooperation regulating the relationship between a NAB and the SA are not a requirement for the accreditation of certification bodies *per se*. However, for reasons of completeness and transparency, the Board considers that such terms of cooperation, where existing, shall be made public in a format considered appropriate by the SA.

2.2.2 GENERAL REMARKS

12. Under the section “terms and definitions” the Board notes that the draft accreditation requirements state that terms and definitions of the EDPB Guidelines on accreditation and Guidelines on certification shall apply and have precedence over ISO definitions, but there is no reference to the definitions used for the same concepts in the GDPR. Thus, the Board recommends the MT SA to also include reference to the terms and definitions of the GDPR.

13. For completeness and consistency purposes, the Board encourages the MT SA to make sure that throughout the requirements the term “target of evaluation” is used in order to ensure clear and consistent wording thorough the text.

2.2.3 GENERAL REQUIREMENTS FOR ACCREDITATION

14. Concerning subsection 4.1.1 of the MT SA's draft accreditation requirements (Legal responsibility), the Board considers that the certification body shall be able to demonstrate evidence of GDPR compliant procedures and measures specifically for controlling and handling client organisation's personal data as part of the certification process. To that end, the Board notes that MT SA refers only to the "applicant" (no reference to the "client" is made), which may be confusing as the same criteria should be applicable for the renewal of accreditation. Therefore, the Board recommends that the MT SA amends the draft requirements accordingly.

15. Also, in this subsection (Legal responsibility), the Board notes the requirement for the certification body to confirm with the NAB that they are not subject to any investigation or regulatory action by the MT SA in relation to the target of evaluation, which may mean that they do not meet this requirement and therefore might prevent their accreditation. This requirement further on provides some ambiguity when it does not give clear criteria (saying "where appropriate") on the situations in which the NAB may contact the MT SA in order to verify this information. To that end, the Board recommends to the MT SA to ensure further clarification and specify clear conditions for this procedure.

16. In addition to that, the Board is of the opinion that subsection 4.1.1 of the MT SA's draft accreditation requirements, regarding the obligation of the certification body to inform the NAB of "any" infringements of the GDPR or of national data protection legislation which may affect its accreditation, should be further clarified, taking into account the above-mentioned requirement that certification body should confirm to the NAB that they are not subject to any investigation or regulatory action by the MT SA in relation to the target of evaluation. Thus, the Board considers that this obligation should refer to infringements established by the MT SA and/or judicial authorities and recommends the MT SA to makes such clarification.

17. Further on, concerning subsection 4.1.1 of the MT SA's draft accreditation requirements, the Board notes that the certification body shall be required to inform the MT SA prior to issuing or renewing a certification and to that end, requirements are referring to Art. 43(1) GDPR. At the same time, the Board notes that the MT SA's draft accreditation requirements in point 7.6 further elaborate this requirement for the certification body. Thus, the Board encourages the MT SA to include in this subsection the reference on the last sentence of point 7.6 of the accreditation requirements, in addition to the already existing one related to Art. 43(1) GDPR.

18. Under section 4.1.2 (i) of the MT SA's draft accreditation requirements, the Board takes note of the obligation to explain the consequences of withdrawal or suspension of accreditation for the certification body and how this impacts the client. The Board understands that the intention of the MT SA is to ensure that the client is aware of the consequences in those situations and of the potential options or actions that can be taken. However, the Board considers that, in order to ensure that certification agreements accurately reflect not only the consequences and impacts on the client, but also the potential further actions, the MT SA's accreditation requirements should make clear that simply stating the consequences without addressing the potential next steps will not be sufficient. Thus, the EDPB encourages the MT SA to make clear in its accreditation requirements that the clients should be aware of the consequences, the impact they have on them and the potential next steps that may be taken.

19. Regarding section 4.1.2 (j) of the MT SA's accreditation requirements, the Board notes the inclusion of the requirement to inform the certification body in the event of significant changes in its factual or legal situation and in its processing operations covered by the certification. However, the MT SA

omitted a reference to "products, processes and services", as stated in the Annex. The Board therefore recommends the MT SA to align the wording with the Annex.

20. Regarding the requirements related to the content of the Certification agreement listed in section 4.1.2, the Board notes that point 10 of section 4.1.2. of the Annex, as reflected in point 4.1.2 (j) of the MT SA's draft requirements, requires the applicant to inform the certification body in the event of significant changes in its actual or legal situation and in its products, processes and services concerned by the certification. The Board considers that these changes shall include the obligation of the applicant to inform the certification body of any infringements of the GDPR established by the MT SA and/or judicial authorities that may affect certification. Indeed, such requirement is foreseen further in the text of the requirements (section 7.10 (e) of the requirements). However, for the sake of clarity, the Board recommends to the MT SA to include explicitly this point in this section of the requirements.

21. With respect to the section 4.2 "Management of impartiality", the Board notes the obligation to lay down rules preventing conflicts of interest. The Board acknowledges the importance to have requirements that ensure, firstly, that there are no conflicts of interests and, secondly, in case conflicts of interest are identified, that the certification body manages them. Therefore, the Board encourages the MT SA to clarify that, in addition to having rules preventing conflicts of interest, there should be clear rules to manage identified conflicts of interests.

22. Regarding section 4.6 of the MT SA's draft accreditation requirements, the certification body is required to:

    a. publish and make easily publicly available all versions (current and previous) of the approved criteria used within the meaning of Art. 42(5) GDPR, as well as all certification procedures, generally stating the respective period of validity; and

    b. provide information about complaints handling procedures and appeals is transparent to data subjects and the public pursuant to Art. 43(2)(d) GDPR.

    The Board recommends to the MT SA to add in the requirements that this information shall be provided **at minimum**, according to section 4.6 of the ISO/IEC 17065/2012 and in line with section 4.6 of the Annex.

23. In order to avoid inaccuracies, possible different understandings and interpretations of the requirement for publicly available information relating to complaint handling procedures and appeals, the Board recommends to the MT SA to align the wording of section 4.6 (b) of the MT SA's draft accreditation requirement with the Annex.

2.2.4 RESOURCE REQUIREMENTS

24. Regarding section 6.1 (f) of the MT SA's draft accreditation requirements, with respect to the second bullet point of the subsection relating to the personnel with technical expertise, the Board refers to the sentence by which it is prescribed that "personnel responsible for certification decisions shall demonstrate at least two years professional experience in data protection law". Considering this section of requirements is addressed to the personnel with technical expertise, the Board consider reference to experience in data protection "law" inaccurate and recommends the MT SA to align the wording with the Annex.

25. Also, regarding section 6.1 (f) of the MT SA's draft accreditation requirements, with respect to the third bullet point of the subsection relating to the personnel with legal expertise, the Board refers to

the sentence by which it is prescribed that “personnel responsible for evaluations must demonstrate at least two years of professional experience in data protection law and knowledge and experience in technical data protection”. Considering this section of requirements is addressed to the personnel with legal expertise the Board consider reference to “experience in technical data protection” inaccurate and recommends the MT SA to align the wording with the Annex.

26. As regards the requirements for personnel responsible for evaluations, in subsection related to personnel with technical expertise, the Board recommends the MT SA to refer to professional experience in “technical” data protection.

2.2.5 PROCESS REQUIREMENTS

27. Taking into account that section 7 of the MT SA’s draft accreditation requirements concerns process requirements and sets certain requirements for the NAB, the Board encourages the MT SA to rephrase section 7.1 (d) in such a way as to replace the words "carries out an investigation" with “have established procedures to investigate”.

28. The Board notes that section 7.2 of the MT SA’s draft accreditation requirements (“Application”) concerns obligations imposed on the applicants towards the certification body. To that end, the Board recommends to the MT SA to rephrase the first paragraph of this section as follows: “In addition to clause 7(2) of ISO 17065, the certification body shall require from the applicant to […]"

29. The Board notes that section 7.2 of the MT SA’s draft accreditation requirements (“Application”) contains a reference to the controller/processor contract(s) and their specific arrangements. While acknowledging that the MT SA has used the wording of the Annex, the Board encourages the MT SA to include a reference to joint controllers and their specific arrangements.

30. Furthermore, the Board recommends to the MT SA to rephrase the section 7.2 (c) in a way to delete the reference to “the certification body” so that it is clear from the text that this obligation primarily refers to the applicant’s obligation during the application stage and fulfilment of which should be checked by the certification body.

31. Regarding section 7.2 (c) (“Application”) of the MT SA’s draft accreditation requirements, the Board notes that it includes the obligation to provide information regarding “any current investigation or regulatory action of the Malta SA to which the applicant is or has been subject”. The Board is of the opinion that this obligation should be tailored to investigations or regulatory actions related to the scope of the certification and the target of evaluation. Therefore, the Board encourages the MT SA to clarify that the investigation or regulatory action should be related to the scope of certification and the target of evaluation.

32. The Board notes that the clarification on the requirement relating to the data protection certification in accordance with Art. 42 and 43 GDPR, which already covers part of the object of certification, according to which “a certification statement or similar certification certificates should not be considered sufficient to replace a report” (section 7.4 of the Annex) is not included in the MT SA’s draft requirements. Thus, the Board recommends that the MT SA includes it in the requirement.

33. Concerning third paragraph of the section 7.6 of the MT SA’s draft accreditation requirements (“Certification decision”), the Board notes that the certification body shall be required, in addition to the checks carried out at application stage, prior to issuing certification, to confirm with the applicant that they are not the subject of any investigation or regulatory action by the MT SA, by any other

supervisory authority and, or by competent judicial authorities in relation to the object of the certification which might prevent certification being issued. Further in the text it is foreseen that the applicant's statement can be confirmed with the MT SA not only prior to issuing, but also prior to the renewing of certification. Therefore, the Board encourages that the MT SA amends this inconsistency.

34. Regarding first paragraph of the section 7.8 of the MT SA's draft accreditation requirements ("Directory of certified product") the Board notes the requirement that records of the certifications issued, including information about the certification mechanism and how long the certifications are valid for shall be publicly available and thus, in principle, it could be concluded that this implies an requirement to keep this information also internally but at the same time, for the purpose of consistency and clarity, Board encourages MT SA to align the wording with the Annex.

35. In addition, the Board notes that this section contains clear requirements aimed at helping with transparency on what has been certified and how it was assessed, to that end, for the purpose of clarity and alignment with Annex the Board encourages the MT SA to delete the words "on which basis" from the first paragraph of the section 7.8.

36. In order to ensure clarity, the Board encourages the MT SA to align the wording in section 7.10 (c) and (d) of the draft accreditation requirements with the Annex.

3 CONCLUSIONS / RECOMMENDATIONS

37. The draft accreditation requirements of the MT Supervisory Authority may lead to an inconsistent application of the accreditation of certification bodies and the following changes need to be made:

38. Regarding 'general remarks', the Board recommends that the MT SA:

    1) includes references to the terms and definitions of the GDPR

39. Regarding 'general requirements for accreditation', the Board recommends that the MT SA:

    2) amend subsection 4.1.1 in line with the remarks made in paragraphs 13 and 14 of the Opinion;

    3) makes clarification in subsection 4.1.1 of the draft accreditation requirements that the obligation of the certification body to inform the NAB on infringements of the GDPR should refer to infringements established by the MT SA and/or judicial authorities in relation to the target of evaluation;

    4) align the wording of section 4.1.2 (j) of the accreditation requirements with the Annex;

    5) include the point relating to applicant informing the certification body of any infringements of the GDPR established by the MT SA and/or judicial authorities that may affect certification in subsection 4.1.2 of the requirements;

    6) align the wording of section 4.6 (b) with the Annex.

40. Regarding 'resource requirements', the Board recommends that the MT SA:

    1) align the wording of second bullet point of the section 6.1 (f) relating to the personnel with technical expertise with the Annex;

2) align the wording of third bullet point of the section 6.1 (f) relating to the personnel with legal expertise with the Annex;

3) align the wording of third bullet point of the section 6.1 (f) of the subsection relating to the personnel with technical expertise with the Annex.

41. Regarding 'process requirements', the Board recommends that the MT SA:

1) amend section 7.2 in line with the remarks made in paragraphs 27 and 29 of this Opinion

2) to include in draft accreditation requirements the sentence of section 7.4 of the Annex which stipulates that "a certification statement or similar certification certificates should not be considered sufficient to replace a report".

3) amend section 7.6, third paragraph of the draft accreditation requirements in a way which clearly points that the intended procedure applies also to the renewing of certification.

4 FINAL REMARKS

42. This opinion is addressed to the MT SA and will be made public pursuant to Art. 64 (5)(b) GDPR.

43. According to Art. 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.

44. 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 Art. 70 (1) (y) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)