Opinion 21/2020 on the draft decision of the competent supervisory authority of the Netherlands regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)

Adopted on 23 July 2020

Table of contents

1 Summary of the Facts 4
2 Assessment 4
2.1 General reasoning of the EDPB regarding the submitted draft decision 4
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: 5
2.2.1 GENERAL REMARKS 6
2.2.2 GENERAL REQUIREMENTS FOR ACCREDITATION 6
2.2.3 RESOURCE REQUIREMENTS 7
2.2.4 PROCESS REQUIREMENTS 8
2.2.5 MANAGEMENT SYSTEM REQUIREMENTS 9
2.2.6 FURTHER ADDITIONAL REQUIREMENTS 9
3 Conclusions / Recommendations 9
4 Final Remarks 10

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 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 Dutch supervisory authority (hereinafter "NL SA") has submitted its draft accreditation requirements under Article 43 (1)(b) to the EDPB. The file was deemed complete on 28 May 2020. The NL national accreditation body (NAB) will perform accreditation of certification bodies to certify using GDPR certification criteria. This means that the NAB will use ISO 17065 and the additional requirements set up by the NL SA, once they are approved by the NL SA, following an opinion from the Board on the draft requirements, to accredit certification bodies.

2 ASSESSMENT

2.1 General reasoning of the EDPB regarding the submitted draft decision

2. 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 article 43(1) GDPR, to accredit a certification body responsible for issuing and renewing certification in accordance with article 42 GDPR. This is without prejudice to the tasks and powers of the competent SA. In this specific case, the Board notes that the NL SA has decided to resort to its national accreditation body (NAB) for the issuance of accreditation, having put together additional requirements in accordance with the Guidelines, which should be used by its NAB when issuing accreditation.

3. This assessment of NL 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

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

Opinion is also focused on all aspects that may impact on a consistent approach regarding the accreditation of certification bodies.

4. 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.

5. 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.

6. The Board notes that ISO standards, in particular ISO 17065, are subject to intellectual property rights, and therefore it will not make reference 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 Standards, without, however, reproducing the text.

7. 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 NL SA's draft accreditation requirements, it should be read as the Board not having any comments and not asking the NL SA to take further action.

8. This opinion does not reflect upon items submitted by the NL SA, which are outside the scope of article 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.

9. Taking into account that:

a. Article 43 (2) GDPR provides a list of accreditation areas that a certification body needs 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 GENERAL REMARKS

10. The Board acknowledges that the NL SA's draft accreditation requirements includes a section on terms and definitions. However, some of the terms are not used consistently throughout the document (e.g. "object of evaluation" and "ToE", the "accreditation body" and "RvA", the term "CB" is not used in the text, the text sometimes refers to "the competent supervisory authority" instead to the "NL SA"...). Additionally, the Board considers that, when referring to the ISO 17065, the relevant section should be mentioned. Whereas this is the case sometimes (e.g. sections 7.3, 7.5, 7.6, 7.7 and 7.9 of the NL SA's draft requirements), it is not consistent throughout the document (e.g. sections 4.2, 4.3, 4.6, 6.2, 7.1, 7.2, 7.4 and 7.8 of the NL SA's draft requirements does not mention the relevant sections of ISO 17065). The Board encourages the NL SA to ensure that the terms used are consistent and that the references to the ISO 17065 are clear.

11. The Board notes that some sections of the Annex are missing (e.g. section 9.3.2 of the Annex "Documentation of evaluation activities"). The Board understands that, in those cases, no additional requirements were formulated. However, for the sake of clarity, the Board encourages the NL SA to either add the missing sections or include a statement at the beginning of the draft requirements, clarifying that, when some sections are missing, it means that no additional requirements were formulated.

2.2.2 GENERAL REQUIREMENTS FOR ACCREDITATION

12. The Board notes that the last paragraph of subsection 4.1.1 of the NL SA's draft accreditation requirements ("Legal responsibility") refers to investigations or regulatory actions in relation to the subject matter of the ToE "*which may mean they do not meet this requirement and therefore might prevent their accreditation."* The Board considers that the last part of the sentence is redundant and

might lead to confusion. Therefore, the Board encourages the NL SA to delete the sentence from "which may mean..."-" prevent their accreditation".

13. With regard to subsection 4.1.2 of the NL SA's draft accreditation requirements ("Certification agreement"), the Board notes that point 6 does not include all the elements of point 8 of the Annex In particular, the "the necessary precautions for the investigation of complaints" are missing. The Board recommends the NL SA to include the missing information from the Annex.

14. Additionally, the Board is of the opinion that point 7 of subsection 4.1.2, regarding to the obligation of the application to inform the certification body of relevant infringements of the GDPR or the UAVG should be clarified. The Board considers that this obligation should not lead to self-incrimination and, therefore, the obligation should refer to infringements established by the NL SA and/or judicial authorities. Thus, the Board recommends the NL SA make such clarification. Moreover, in order to avoid confusion, the Board encourages the NL SA to clarify that "relevant infringements" refer to infringements of the GDPR or the UAVG that may affect certification.

15. Regarding point 9 of subsection 4.1.2, the Board notes the inclusion of a reference to the consequences for the data subjects. However, the NL SA omitted a reference to [where applicable] "the consequences for the customer should also be addressed", as stated in the Annex. The Board therefore recommends the NL SA to replace the term with "customer", in order to align the wording with the Annex.

16. With regard to section 4.3 ("Liability and financing") of the NL SA's draft accreditation requirements, the Board notes that, in accordance with the Annex, the certification body shall demonstrate on a regular basis that it has the appropriate measures to cover its liabilities. The NL SA's draft accreditation requirements do not include the notion of "regular basis" and, therefore, the Board recommends the NL SA to include such reference, in line with the Annex.

17. The Board notes that section 4.3 of the NL SA's draft accreditation requirements contains the obligation to having adequate financial resources to demonstrate how the fines, that may be imposed under article 83(4)(b) GDPR, will be paid. The Board considers that this specific reference to the fines under GDPR may lead to some difficulties in practice, especially with regard to the assessment of compliance with the requirements. Thus, the Board encourages the NL SA to reconsider the specific reference to fines under GDPR, taking into account the potential practical difficulties that such reference may imply.

18. The Board notes that section 4.6 of the NL SA's draft accreditation requirements ("Publicly available information") includes the obligation to demonstrate the publication of the approved criteria and "high-level explanations about the certification procedures". The Board notes that a "high-level" explanation may not be enough to provide the information required in the Annex. Therefore, the Board encourages the NL SA to add that "meaningful" explanations will be provided.

2.2.3 RESOURCE REQUIREMENTS

19. Concerning certification body personnel (section 6.1 of the NL SA'S draft accreditation requirements), the Board notes that the requirements follow the Annex. In this respect, the Board is of the opinion that, with regard to the expertise of the certification body, the emphasis should be put on the different type of substantive expertise and experience. Specifically, the Board considers that the competence requirements for evaluators and decision-makers should be tailored taking into account the different tasks that they perform. In the Board's opinion, evaluators should have a more specialist expertise

and professional experience in technical procedures (e.g. audits and certifications), whereas decision-makers should have a more general and comprehensive expertise and professional experience in data protection. Considering this, the Board encourages the NL SA to redraft this section taking into account the different substantive knowledge and/or experience requirements for evaluators and decision-makers.

20. Additionally, the Board notes that, with regard to personnel with legal expertise, the Annex requires a specific educational background or significant professional experience. This last reference is missing in the NL SA's draft accreditation requirements. The Board recommends the NL SA to add such reference.

21. Moreover, regarding the education requirements for technical expertise, the Annex refers to "a qualification in a relevant area of technical expertise to at least EQF level 6 or a recognised protected title (e.g. Dipl. Ing.) in the relevant regulated profession". The Board notes that the NL SA's draft accreditation requirements does not include the reference to the recognised title and encourages the NL SA to include such reference.

2.2.4 PROCESS REQUIREMENTS

22. Regarding section 7.2 ("Application") of the NL SA's draft accreditation requirements, the Board notes that point 4 includes the obligation to "*disclose any current or recent AP investigation or regulatory action to which the applicant is subject"*. The Board is of the opinion that the 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 NL SA to clarify that the investigation or regulatory action should be related to the scope of certification and the target of evaluation.

23. With regard to section 7.4 ("Evaluation"), point 3, the Board considers that the reference to the requirements "as set out in the criteria" seems to presuppose that the criteria are complete. While acknowledging that the NL SA has used the wording of the Annex, the Board encourages the NL SA to refer to "the adopted criteria", in order to avoid confusion.

24. The Board notes that the second paragraph of section 7.6 of the NL SA's draft accreditation requirements ("certification decision") includes the obligation to submit the draft approval to the NL SA, prior to issuing or renewing certification. Based on the explanations provided by the NL SA, the Board understands that the intention of this requirement is to increase transparency and it does not entail a supervision of the draft approval. The Board encourages the NL SA to include a clarification in that sense.

25. With regard to section 7.10 of the NL SA's draft accreditation requirements ("Changes affecting certification"), the Board notes that the first bullet point includes "any personal data breach or infringement of the GDPR". The Board considers that, in order to avoid self-incrimination, the reference should be to infringements established by the NL SA or the competent judicial authority. Additionally, the reference to "any data breach" seems quite broad. The Board is of the view that such reference should be further developed, in order to clarify whether minor data breaches should also be reported. Therefore, the Board encourages the NL SA to change the wording, by referring to "established" infringements and clarify the meaning of "any data breach".

26. The Board notes that the first sentence of section 7.11 is not formulated as a mandatory requirement. The Board encourages the NL SA to replace the word "should" by "shall", to make clear that it is an

obligation. Additionally, the Board notes that the obligation to inform about measures taken is also towards the NAB, as stated in the Annex. The Board recommends the NL SA to add such reference to the NAB.

27. Finally, section 7.13 of the NL SA's draft accreditation requirements ("Complaints and appeals"), states the obligation to inform the complainant of the progress and the outcome of the complaint within one month of receipt of the complaint. Whereas transparency towards complainants is of great importance, the Board considers that a strict obligation to provide the complainant the outcome of the complaint in one month may create unrealistic expectations and pose a high challenge for the certification body. Therefore, the Board encourages the NL SA to redraft the requirements by stating that the certification body has to inform the complainants of the progress or the outcome within one month of receipt of the complaint.

2.2.5 MANAGEMENT SYSTEM REQUIREMENTS

28. With regard to section 8 of the NL SA's draft accreditation requirements ("Management system requirements"), the Board notes that the obligation of the certification body to disclose to the NL SA the management principles and their documented implementation during the accreditation procedure is not foreseen. The Board recommends the NL SA to amend the draft requirements, by including such obligation, as stated in the Annex.

2.2.6 FURTHER ADDITIONAL REQUIREMENTS

29. Section 9.3.2 of the NL SA's draft accreditation requirements ("Management of complaint handling") does not include the obligation to share with the NL SA relevant complaints and objections, as stated in the Annex. The Board recommends the NL SA to include such obligation.

3 CONCLUSIONS / RECOMMENDATIONS

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

31. Regarding 'general requirements for accreditation', the Board recommends that the NL SA:

    1) Add the missing information from the Annex references in point 6 of subsection 4.1.2.

    2) clarify in point 7 of subsection 4.1.2 that the the obligation of the applicant to inform the certification body of relevant infringements of the GDPR or the UAVG should refer to infringements established by the NL SA and/or judicial authorities.

    3) replace in point 9 of subsection 4.1.2 the term with "customer", in order to align the wording with the Annex.

    4) include in section 4.3 the reference to the notion of "regular basis", in line with the Annex.

32. Regarding 'resource requirements', the Board recommends that the NL SA:

    1) add in section 6.1 the reference to significant professional experience with regard to personnel with legal expertise

33. Regarding ‘process requirements’, the Board recommends that the NL SA:

    1) add in section 7.11 the obligation to inform the NAB about measures taken, in line with the Annex.

34. Regarding ‘management system requirements’, the Board recommends that the NL SA:

    1) include in section 8 the obligation to disclose to the NL SA the management principles and their documented implementation during the accreditation procedure.

35. Regarding ‘further additional requirements’, the Board recommends that the NL SA:

    include in subsection 9.3.2 the obligation to share with the NL SA relevant complaints and objections, as stated in the Annex

4 FINAL REMARKS

36. This opinion is addressed to the Dutch Supervisory Authority and will be made public pursuant to Article 64 (5)(b) GDPR.

37. According to Article 64 (7) and (8) GDPR, the NL SA shall communicate to the Chair by electronic means within two weeks after receiving the opinion, whether it will amend or maintain its draft list. Within the same period, it shall provide the amended draft list 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.

38. The NL 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)