Opinion 26/2020 on the draft decision of the competent supervisory authority of Denmark regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)

Adopted on 07 December 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 REQUIREMENTS FOR ACCREDITATION (Section 4 of the draft accreditation requirements) 6
2.2.2 RESOURCE REQUIREMENTS (Section 6 of the draft accreditation requirements) 7
2.2.3 Process requirements, Article 43 (2)(c), (d) of the GDPR (Section 7 of the draft accreditation requirements) 7
3 Conclusions / Recommendations 8
4 Final Remarks 8

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 Danish Supervisory Authority (hereinafter "DK SA") has submitted its draft accreditation requirements under Article 43 (1)(b) to the EDPB. The file was deemed complete on 12 October 2020. The Danish 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 DK SA, once they are approved by the DK 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 DK SA, although empowered together with the Danish Accreditation Fund (DANAK) to grant accreditation to certification bodes, has decided to resort to DANAK, i.e. 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.

[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

3. This assessment of DK 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.

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

8. This opinion does not reflect upon items submitted by the DK 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 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 GENERAL REQUIREMENTS FOR ACCREDITATION (Section 4 of the draft accreditation requirements)

10. With regard to paragraph 3 in section 4.1.1 "Legal responsibility" of the DK SA's draft accreditation requirements, the Board is of the opinion that the certification body should confirm to the accreditation body not only that fact that they are not subject of any investigation or regulatory action by the DK DPA, but also that they were not subject of such investigation/regulatory action in the past. Therefore, the Board encourages the DK SA to clarify this matter.

11. With respect to the same section, last paragraph, the Board encourages DK SA to make clear that further requirements and procedures aimed at checking certification bodies GDPR compliance prior to accreditation can be added.

12. The Board underlines the importance of full transparency by the certification body to the DK DPA with respect to the certification procedure. In this context, as regards section 4.1.2 certification agreement, paragraph 2, the Board encourages DK SA to specify what is meant by the term "otherwise", in particular whether confidentiality imposed by the law is covered by this provision.

13. With respect to the section 4.2 "Management of impartiality", the Board encourages DK SA to provide more examples of situations where certification body has no relevant connection with the customer

it assesses. In particular, requirements for accreditation of a certification body submitted by German SA and Austrian SA might be of help in this regard[3].

2.2.2 RESOURCE REQUIREMENTS (Section 6 of the draft accreditation requirements)

14. The Board takes good note of the fact that DK SA's accreditation requirements allows for outsourcing of certain activities. With respect to access to someone with relevant expertise, and an appropriate professional/degree level qualification ("Certification body personnel", section 6.1.6), the Board recommends to the DK SA to clearly underline that the certification body will retain the responsibility for the decision-making, even when it uses external experts[4]. The Board highlights that external actors should not be involved in decision making process and that this needs to be clearly underlined in the requirements.

15. As regards the same section and the reference to personnel responsible for certification decisions, the Board encourages DK SA to align the wording of the requirements with the wording of the Guidelines, by adding a reference to data protection laws, i.e. "significant professional experience in data protection law, including identifying and implementing data protection measures".

2.2.3 Process requirements, Article 43 (2)(c), (d) of the GDPR (Section 7 of the draft accreditation requirements)

16. With respect to section 7.2 "Application" and the requirement to notify DK DPA about an application received, the Board encourages DK SA to specify in the last sentence in which form the notification should be submitted by the certification body.

17. As regards section 7.4 "Evaluation", third paragraph, the Board recommends to DK SA to add not only the respective requirements of ISO 17065 but also the additional ones of the Danish DPA, which must be fulfilled by the sub-contractor, as well as to underline that sub-contracting does not exempt the certification body from its responsibilities.

18. Regarding section 7.6 "Certification decision", the Board underlines that the certification body should in detail set out procedures how its independence and responsibility are ensured. For this reasons the Board recommends to DK SA to add at the beginning of point 7.6 "Certification decision" the following sentence: "In addition to point 7.6.1 of ISO/IEC 17065/2012, the certification body should be required

[3] For possible examples see Opinion 15/2020 on the draft decision of the competent supervisory authorities of Germany regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR) - section 19 or Opinion 9/2019 on the Austrian data protection supervisory authority draft accreditation requirements for a code of conduct monitoring body pursuant to article 41 GDPR - section 20.

[4] The EDPB developed this requirement in Opinion 16/2020 on the draft decision of the competent supervisory authority of the Czech Republic regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR) - see section 24; and Opinion 5/2020 on the draft decision of the competent supervisory authority of Luxembourg regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 GDPR - see section 14.

to set out in detail in its procedures how its independence and responsibility with regard to individual certification decisions are ensured".

19. The Board underlines the importance of providing information about reasons for granting or revoking certification. For this reason, the Board recommends DK SA to add in section 7.8 "Directory of certified products", the reference to the duty for the certification body to inform about granting/revoking requested certification including clarification in which form such information should be provided.

3 CONCLUSIONS / RECOMMENDATIONS

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

21. Regarding 'resource requirements', the Board recommends that the DK SA:

    1) in section 6.1.6 "Certification body personnel", clearly underline that the certification body will retain the responsibility for the decision-making, even when it uses external experts;

22. Regarding 'process requirements', the Board recommends that the DK SA:

    1) in section 7.4 "Evaluation", third paragraph, add not only the respective requirements of ISO 17065 but also the additional ones of the Danish DPA, which must be fulfilled by the sub-contractor, as well as underline that sub-contracting does not exempt the certification body from its responsibilities;
    2) in section 7.6 "Certification decision" add the following sentence: "In addition to point 7.6.1 of ISO/IEC 17065/2012, the certification body should be required to set out in detail in its procedures how its independence and responsibility with regard to individual certification decisions are ensured";
    3) in section 7.8 "Directory of certified products", add a reference to the duty for the certification body to inform about granting/revoking requested certification including clarification in which form such information should be provided.

4 FINAL REMARKS

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

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

25. The DK 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)