Opinion 35/2021 on the draft decision of the competent supervisory authority of Belgium regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)

Adopted on 30 November 2021

Adopted

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 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 Belgian supervisory authority (hereinafter "BE SA") has submitted its draft accreditation requirements under Article 43 (1)(b) to the EDPB. The file was deemed complete on 5 October 2021. The BE 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 BE SA, once they are approved by the BE SA, following an opinion from the Board on the draft requirements, to accredit certification bodies. The BE SA will perform accreditation of certification bodies to certify using GDPR certification criteria]

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 BE 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.

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

8. This opinion does not reflect upon items submitted by the BE 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 PREFIX

10. The Board acknowledges the fact that terms of cooperation regulating the relationship between a National Accreditation Body and its data protection supervisory authority 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

11. Under the same section "terms and definitions" the Board encourages the BE SA to complete the GDPR definition as follows "*Regulation (EU) 2016/679 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".* Similarly, the Board encourages the BE SA to remove the "*and/or by a supervisory authority"* from the definition of terms and definitions.

12. For completeness and consistency purposes, the Board encourages the BE SA to make sure that where throughout the requirements there is a reference to a section of ISO, to ensure that the relevant ISO is mentioned (e.g. 7.3.(2) the reference to ISO 17065 is missing).

13. The Board encourages the BE SA to ensure the consistency of terms, such as "shall" throughout the entire draft accreditation requirements and to make sure that all the "should" have been replaced with "shall" (e.g. in Section 9.3.4 "*relevant complaints and objections should be shared with the Belgian DPA*" and section 7.6. "*In addition to item 7.6.1 of ISO 17065, the certification body should be required [...]*").

Similarly, the Board encourages the BE SA to replace under section 7.4. of the draft requirements the term "existing certification" with the term " data protection certification".

Adopted

2.2.3 GENERAL REQUIREMENTS FOR ACCREDITATION

14. In addition, 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 BE SA to clarify that, in addition to having rules preventing conflicts, there should be clear rules to manage identified conflicts of interests.

15. With respect to the section 4.2 "Management of impartiality", the Board encourages the BESA to provide more examples of situations where certification body has no relevant connection with the customer it assesses (e.g. the non-existence of a contractual relationship between the certification body and the customer). The Board takes note of the obligation, as provided under section 4.1.2 (9), that if the consequences of withdrawal or suspension of accreditation of the certification body has an impact on the client, the consequences must be addressed. The Board notes the obligation to address consequences that may impact the client. However, for the Board it is not entirely clear that there is an obligation to ensure that the client is aware of such consequences. Therefore, the Board encourages the BE SA to redraft the requirement so to make clear that the client should be informed of consequences that affect him/her.

16. Similarly, the Board takes note that the potential options or actions to be taken in the above mentioned case are missing from the BE SA's accreditation requirements. 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 BE 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 BE 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.

2.2.4 RESOURCE REQUIREMENTS

17. Moreover, the Board considers that the expertise requirements for evaluators and decision-makers should be tailored taking into account the different tasks that they perform. In this regard, the Board is of the opinion that 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 BE SA to redraft the requirements taking into account the different substantive knowledge and/or experience requirements for evaluators and decision-makers. With regard to the reference to the knowledge of decision-makers of the ISO 17065 and the additional accreditation requirements, the Board notes that the same requirement could be applicable to personnel in charge of evaluation, and encourages the BE SA to amend the draft accordingly.

2.2.5 PROCESS REQUIREMENTS

18. The Board notes that under section 7.4 of the draft accreditation requirements, the BE SA makes reference to the possibility that the evaluation is carried out by subcontractors. The Board recommends the BE SA to clearly underline that the certification body will retain the responsibility for the decision-making, even if it uses external experts. 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.

Adopted

19. The Board takes note of the general process requirements, as listed in section 7.1 of the BE SA's draft accreditation criteria. However, the EDPB highlights that the obligation of the accreditation body to notify the relevant CSAs before a certification body starts operating an approved EU Data Protection Seal in a new Member State is missing. Therefore, the Board recommends that the BE SA modifies its requirements accordingly so to bring section 7.1(2) of the latter in line with the section 7.1(2) of the Guidelines.

20. The Board notes that the section 7.6 of the BE SA's draft requirements, includes the obligation to submit the draft approval to the BE SA, prior to issuing or renewing certification. The Board understands that the intention of this requirement is to increase transparency and it does not entail a supervision of the draft approval by the Supervisory Authority, without prejudice to its power of Article 58(2)(h) GDPR. The Board encourages the BE SA in include a clarification thereof in the relevant section of its accreditation requirements.

21. The Board observes that under section 7.8 of the BE SA's accreditation requirements, the obligation to inform the competent SA of the reasons for granting or revoking the requested certification is missing. According to the section 7.8 of the Annex to the Guidelines, there is an obligation to proactively inform the SA of the reasons for granting or revoking the certification. Therefore, the Board recommends the BE SA to amend this requirement accordingly.

22. In addition, the Board underlines the importance of providing information about the reasons for granting or revoking certification. For this reason, the Board recommends the BE SA to add in section 7.8 of its accreditation requirements, the reference to the duty for the certification body to inform about granting or revoking the requested certification including clarification in which form such information should be provided.

23. Pursuant to section 7.11 of the Annex to the Guidelines, the certification body should be required to inform the competent SA and the NAB about measures taken regarding the continuation, restrictions, suspensions and withdrawal of the certification. The Board notes that under section 7.11, paragraph 3, the reference to notification of the NAB (in this case BELAC) is missing. Therefore, the Board recommends to amend this requirement by including such reference.

2.2.6 MANAGEMENT SYSTEM REQUIREMENTS

24. Under section 8, there paragraph of the Guidelines (section 8) "In particular, the accredited certification body must make public permanently and continuously which certifications were carried out on which basis (or certification mechanisms or schemes), how long certifications are valid under which framework and conditions (recital 100)". The Board recommends the BE SA to add a recommendation to add this paragraph for consistency with the Guidelines.

3 CONCLUSIONS / RECOMMENDATIONS

25. Regarding 'process requirements', the Board recommends that the BE SA:

    1) modify its requirements to include the notification of the CSAs so to bring section 7.1(2) of the latter in line with the section 7.1(2) of the Guidelines.

    2) clarify that the submission of the draft approval aims at increasing tranparency.

Adopted

3) add a reference to the duty for the certification body to inform about granting or revoking the requested certification including clarification in which form such information.

4) include in which form the provision of information about granting or revoking certification will be provided.

5) include a referece to informing BELAC when it comes to about measures taken regarding the continuation, restrictions, suspensions and withdrawal of the certification (section 7.11 paragraph.3).

26. Regarding 'management system requirements', the Board recommends that the BE SA:

1) add the following wording " *In particular, the accredited certification body must make public permanently and continuously which certifications were carried out on which basis (or certification mechanisms or schemes), how long certifications are valid under which framework and conditions (recital 100)"* to bring the requirements in line with the Guidelines.

4 FINAL REMARKS

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

28. According to Article 64 (7) and (8) GDPR, the BE 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.

29. The BE 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)

Adopted