Opinion 22/2020 on the draft decision of the competent supervisory authority of Greece 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 PREFIX 6

2.2.2 TERMS AND DEFINITIONS 7

2.2.3 GENERAL REMARKS 7

2.2.4 GENERAL REQUIREMENTS FOR ACCREDITATION 7

2.2.5 STRUCTURAL REQUIREMENTS 8

2.2.6 RESOURCE REQUIREMENTS 8

2.2.7 PROCESS REQUIREMENTS 9

2.2.8 FURTHER ADDITIONAL REQUIREMENTS 10

3 Conclusions / Recommendations 10

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 Hellenic Supervisory Authority (hereinafter "EL 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 Greek 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 EL SA, once they are approved by the EL 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 EL 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 EL 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 EL SA's draft accreditation requirements, it should be read as the Board not having any comments and not asking the EL SA to take further action.

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

11. The Board notes that the first point in section 0 of the EL SA's draft accreditation requirements states that "*In particular, the E.SY.D. shall provide the HDPA with a brief description of the request, the name and contact details of the certification body, the certification scheme for which accreditation is requested and whether the certification criteria are approved by the competent supervisory authority or the EDPB, or if their approval is pending*." Based on the explanations provided by the EL SA, the Board understands that the last part of the sentence refers to those situations in which the accreditation application is submitted to the NAB before the certification criteria receive the final approval, but the accreditation will not be given until such approval takes place. In order to avoid confusion, the Board encourages the EL SA to clarify that the accreditation will not be granted until the certification criteria receive the final approval.

12. The Board notes that section 0 of the EL SA's draft accreditation requirements states that "*The HDPA, if it deems appropriate, shall inform the E.SY.D. within a reasonable time of any important reasons for non-compliance by the certification body with the GDPR. Although the E.SY.D. can continue the accreditation process, it shall not conclude it until the HDPA has reached its final decision in this respect."* The Board encourages the EL SA to clarify that the NAB should take into account the decision

taken by the EL SA, although the NAB is free to decide with regard to the granting of accreditation, without prejudice to the power of the EL SA to revoke it afterwards, if appropriate.

2.2.2 TERMS AND DEFINITIONS

13. The Board notes that the reference to the guidelines on accreditation as "WP 261" is not updated. The EDPB adopted the Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679). Therefore, the Board encourages the EL SA to amend the wording and refer to the Guidelines 4/2018.

2.2.3 GENERAL REMARKS

14. The Board notes that some terms are not used consistently (e.g. reference to "competent SA" instead to the "EL SA" in some requirements, such as point 3 of subsection 4.1.2). Additionally, the Board considers that, when referring to a specific section of the ISO 17065 or Article of the GDPR, it should be clear to which of the two the reference is made (e.g. point 8 of subsection 4.1.2 does not make the distinction between the two different references). The Board encourages the EL SA to ensure that the terms used are consistent and that the references to the ISO 17065 and the GDPR are clear.

2.2.4 GENERAL REQUIREMENTS FOR ACCREDITATION

15. The Board notes that section 4.1.1 (legal responsibility) second indent (starting with "Inform the ESYD...") and section 4.1.2 (certification agreement) point 11 of the EL SA's accreditation requirements refer to the obligation to inform about "any infringements" of the GDPR. The Board is of the opinion that such obligation should not lead to self-incrimination and, therefore, the obligation should refer to infringements established by the EL SA and/or judicial authorities. Thus, the Board recommends the EL SA make such clarification.

16. With regard to section 4.1.2 (certification agreement) of the EL SA's draft accreditation requirements, the Board notes that the first paragraph states that the certification agreement shall be "in writing". In order to ensure that electronic certification agreements are also covered, the EDPB encourages the EL SA to replace "in writing" by "in written form" or equivalent wording.

17. Moreover, with regard to point 9 of section 4.1.2 of the EL SA's draft accreditation requirements, the Board acknowledges the inclusion of appropriate procedures "into the management of the certification body". The Board understands that the reference is to the management system and encourages the EL SA to clarify it accordingly.

18. Regarding section 4.1.3 of the EL SA's draft accreditation requirements, the Board acknowledges the obligation to inform the EL SA about the data protection seals and marks and provide a copy. However, the Board is of the opinion that the addressees of such obligation are not clear from the requirement. Therefore, the Board encourages the EL SA to clarify the addressees of the above-mentioned obligation.

19. With regard to the requirements to manage impartiality (section 4.2 of the EL SA's draft accreditation requirements) and, in particular, the reference to the conflict of interests in the last paragraph, the Board considers that the wording should be clarified. The Board acknowledges the importance to have requirements that ensure, firstly, that there are no conflicts of interests and, secondly, in the case that conflicts of interest are identified, that the certification body manages them. The Board is of the

opinion that the wording of the EL SA's draft requirements seems to reverse this logical order. In order to avoid confusion, the Board encourages the EL SA to rephrase the sentence by stating first that the certification body shall ensure that there are no conflicts of interest.

20. The Board notes that indent 2 of section 4.2 of the EL SA's draft accreditation requirements states that the certification body shall not be "affiliated" with the customer it assesses. The Board encourages the EL SA to clarify the wording, in order to reflect the independence of the certification body. For example, the EL SA could state that the certification body should not belong to the same company group nor should be controlled in any way by the customer it assesses.

2.2.5 STRUCTURAL REQUIREMENTS

21. The Board observes that section 5.1 of the EL SA' draft accreditation requirements make reference to the appointment of "a person with significant experience in the protection of personal data with responsibility for overseeing data protection compliance." The functions of this figure seem similar to those of a data protection officer. The Board encourages the EL SA to clearly set out the functions of this figure.

2.2.6 RESOURCE REQUIREMENTS

22. Concerning certification body personnel (section 6.1), 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 EL SA to redraft this section taking into account the different substantive knowledge and/or experience requirements for evaluators and decision-makers.

23. Additionally, regarding the educational requirements of the technical personnel, the Board considers that the list of subjects is already tailored to the technical expertise required by the Annex. Therefore, the Board encourages the EL SA to delete the reference to "natural sciences" from the list of subjects regarding the educational requirements of the technical personnel.

24. Finally, the Board considers that the last paragraph of section 6.1 is applicable to both personnel with technical expertise and with legal expertise. The Board encourages the EL SA to clarify that it includes both.

25. Regarding the educational requirements for personnel with 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". However, there is no reference to the underlined sentence in the EL SA's draft accreditation requirements. Additionally, the reference to the qualification to at least EQF level 6 has been replaced by an explicit reference to a university degree. Taking into account the variety in the educational systems, the Board recommends that the EL SA's draft requirements be aligned with the wording of the Annex, taking into account the specific educational system and requirements established in national law. For example, the requirements

could refer to a qualification "in information technology, computer science or mathematics of at least EQF level 6 or an equivalent vocational education enjoying a recognised protected title in the Member State where it was issued".

2.2.7 PROCESS REQUIREMENTS

26. The Board notes that section 7.2 of the EL SA's draft accreditation requirements ("application") contains a reference to the controller/processor contract(s) and their specific arrangements. While acknowledging that the EL SA has used the wording of the Annex, the Board encourages the EL SA to include a reference to joint controllers and their specific arrangements.

27. 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 EL SA has used the wording of the Annex, the Board encourages the EL SA to refer to "the adopted criteria", in order to avoid confusion.

28. With regard to section 7.8 of the EL SA's draft accreditation requirements ("directory of certified products"), the Board notes that the two paragraphs listing the information that shall be made publicly available seem to overlap, since the relationship between the two documents mentioned (directory and evaluation report) is not clear. The Board encourages the EL SA to clarify the relationship between the two documents mentioned in those paragraphs.

29. Regarding section 7.9 ("Surveillance") of the EL SA's draft accreditation requirements, the Board notes that the periodicity of the surveillance is stated as "at least twice during the certification cycle". The Board considers that, when determining the periodicity of the surveillance, the risk associated with the processing should be taken into account. Therefore, the Board encourages the EL SA to include a risk-based approach with regard to the arrangements for surveillance.

30. Regarding section 7.11 of the EL SA's draft accreditation requirements ("Termination, reduction, suspension or withdrawal of certification), the Board notes that the third paragraph states that, with regard to the obligation to accept the decisions and orders of the EL SA to not issue certification when the requirements for certification are no longer met, *"the certification body shall provide clear and documented evidence to the HDPA that the certification criteria are not being met".* Based on further explanations provided by the EL SA, the Board understands that the obligation of the certification body is to provide evidence to the EL SA that proper action has been taken. The Board encourages the EL SA to clarify the meaning in those lines.

31. Additionally, the Board notes and welcomes the inclusion of a requirement related to serious data breaches. However, in order to avoid confusion, the Board encourages the EL SA to clarify that such requirement do not affect the obligation of the clients to inform the SA in accordance to the GDPR.

32. Finally, the Board notes that section 7.12 ("Records") of the EL SA's draft accreditation requirements includes the obligation to record the contact details of certification body personnel responsible for evaluation and certification decisions, and to make such information available to the EL SA upon request. The Board is of the opinion that the ultimate responsible for the activities of the certification body's personnel is the certification body. Therefore, the Board encourages the EL SA to specify the purpose of the requirement.

2.2.8 FURTHER ADDITIONAL REQUIREMENTS

33. Regarding subsection 9.3.1 ("Communication between CB and its clients"), the Board notes that the EL SA's draft accreditation requirements include the obligation to have procedures in place for implementing appropriate procedures and communication structures between the certification body and its clients. In section 3 ("Terms and definitions") of the EL SA's draft accreditation requirements, "client" is described as "the controller of processor that has been certified". However, the requirements in subsection 9.3.1 of the EL SA's draft accreditation requirements are also relevant for applicants and, therefore, the Board encourages the EL SA to clarify it.

34. The Board notes that the last paragraph of subsection 9.3.3 is not formulated as a mandatory requirement. The Board encourages the EL SA to replace the word "should" by "shall", to make clear that it is an obligation. Additionally, the Board considers that relevant complaints and objections not only have to be notified to the EL SA, but they have to be shared with the EL SA. The obligation to share with the EL SA the relevant complains and objections shall be clear in the requirements. Therefore, the Board recommends the EL SA to redraft the requirement by stating that relevant complaints and objections shall be shared with the EL SA.

3 CONCLUSIONS / RECOMMENDATIONS

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

36. Regarding 'general requirements for accreditation', the Board recommends that the EL SA:

    1) clarify in sections 4.1.1 and 4.1.2 that the obligation to inform about any infringements of the GDPR refers to infringements established by the EL SA and/or judicial authorities.

37. Regarding 'resource requirements', the Board recommends that the EL SA:

    1) align the wording regarding the education requirements for personnel with technical expertise with the Annex, taking into account the specific educational system and requirements established in national law.

38. Regarding 'further additional requirements', the Board recommends that the EL SA:

    1) redraft the requirement in subsection 9.3.3 by stating that relevant complaints and objections shall be shared with the EL SA.

4 FINAL REMARKS

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

40. According to Article 64 (7) and (8) GDPR, the EL 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.

41. The EL 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)