Opinion 12/2023 on the draft decision of the competent supervisory authority of Cyprus regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)

Adopted on 11 July 2023

Table of contents

The European Data Protection Board

Having regard to Article 63, Article 64 (1c), (3) - (8) and Article 43 (3) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018, [1]

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

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

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

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

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

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

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

limited to, the requirements detailed in Article 43(2). In comparison to the obligations relating to the accreditation of certification bodies by national accreditation bodies, Article 43 provides fewer details about the requirements for accreditation when the supervisory authority conducts the accreditation itself. In the interests of contributing to a harmonised approach to accreditation, the accreditation requirements used by the supervisory authority should be guided by ISO/IEC 17065 and should be complemented by the additional requirements a supervisory authority establishes pursuant to Article 43(1)(b). The EDPB notes that Article 43(2)(a)-(e) reflect and specify requirements of ISO 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 Cypriot (hereinafter "CY SA") has submitted its draft accreditation requirements under Article 43 (1)(b) to the EDPB. The file was deemed complete on16 May 2023. The CY national accreditation body (NAB) will perform accreditation of certification bodies to certify using GDPR certification criteria pursuant to Article 43 GDPR. This means that the NAB will use ISO 17065 and the additional requirements set up by the CY SA, once they are approved by the CY SA, following an opinion from the Board on the draft requirements, to accredit certification bodies. The accreditation will be issued by the NAB after a favorable opinion provided by the CY SA according to the national law. [3]

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

[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] Law providing for the protection of natural persons with regard to the processing of personal data and for the free movement of such data, Law 125(I)/2018)

3. This assessment of CY 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 CY SA's draft accreditation requirements, it should be read as the Board not having any comments and not asking the CY SA to take further action.

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

9. This Opinion does not reflect upon the terms of cooperation of the CY SA with the NAB, as included in the "Prefix" Section of CY SA's draft accreditation requirements.

1.2 Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently:

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

b. independence of the certification body

c. conflicts of interests of the certification body

d. expertise of the certification body

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

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

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

10. Taking into account that:

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

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

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

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

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

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

the Board is of the opinion that:

1.2.1 PREFIX

11. 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.

1.2.2 GENERAL REMARKS

12. The Board notes that there are some typos throughout the text of the CY SA's draft accreditation requirements (e.g. section 3, 2016/679/EC instead of (EU)) and thus encourages the CY SA to ensure that such typos will be corrected as appropriate.

13. The Board notes that the CY SA, in some parts of the draft requirement, makes use of the term "should" instead of "shall". The Board encourages the CY SA to replace the term "should" with "shall" so to ensure that the requirements are mandatory as appropriate, taking into account the Guidelines. As an example, this change should be made in section 4.1.2 of the draft accreditation requirements, number 9.

1.2.3 GENERAL REQUIREMENTS FOR ACCREDITATION

14. With respect to section 4.1.1. of the CY SA's draft accreditation requirements "the certification body shall be able to demonstrate evidence of the GDPR compliance at any time during the accreditation

process". At the sentence right above it is mentioned "As the certification body is a data controller/processor itself, it shall be able to demonstrate evidence of the GDPR and Law 125(I)/2018 compliant procedures and measures specifically for controlling and handling of client organization's personal data as part of the certification process". To avoid confusion and repetition, the Board encourages the CY SA to remove the first sentence from the requirements.

15. Regarding the consistency of the terminology, the Board encourages the CY SA to use the term "requirement(s)" consistently throughout the text (e.g. section 6.2. to replace the term "conditions" with the term "requirement") so to avoid confusion.

1.2.4 RESOURCE REQUIREMENTS

16. Regarding section 6.1 "certification body personnel" and in particular the personnel with technical expertise, the Board takes note of the insertion of "Must have obtained a degree in information technology, computer science or mathematics of at least EQF level 6 from a Cypriot, Greek or a foreign university or an equivalent vocational education enjoying a recognized protected title in the Member State where it was issued". The Board recommends that the CY SA to amend this requirement, by replacing the term "degree" with the term "qualification" in order to bring it line with the Guidelines.

17. With respect to the same paragraph of this section, the Board recommends the CY SA to align the wording with this of the Guidelines. In particular, the Board recommends the CY SA, to add, in addition to the "relevant professional experience", that this experience must also be significant.

18. In section 6.1., concerning personnel with legal expertise, the CY SA mentions "Personnel responsible for certification decisions shall demonstrate at least two years of professional and comprehensive experience and expertise in certification measures related to data protection law". The Board encourages the CY SA to re-draft this requirement to reflect that the experience and expertise are related to the sector of certification measures with regards to data protection law.

19. In addition, in the same section (bullet point 3), the Board recommends the CY SA, in order to bring this requirement in line with the Guidelines, to replace the term "technical" procedures with the term "comparable".

1.2.5 PROCESS REQUIREMENTS

20. In section 7.1, point 3 the CY SA states "that certification bodies have established procedures to examine that the procedures and mechanisms of the applicant for processing and handling personal data related to the scope of the certification and the ToE are compliant with the GDPR;" The Board understands that the terms "scope of certification" and "ToE" have the same meaning, thus the Board encourages the CY SA to delete one of the two terms so to avoid confusion.

21. Concerning point 4 of the same section, the Board encourages the CY SA to delete the word "requested" before the word certification so to avoid confusion.

22. Regarding section 7.2 "application" of the draft accreditation requirements, the Board takes note of the fact that the certification body shall provide a short description to the CY SA of each one of the applications. The Board welcomes this insertion, however it encourages the CY SA to clarify that what this short description what the CY SA wants to receive entails.

23. As regards to section 7.11 "termination, reduction, suspension or withdrawal of certification" the CY SA refers to non-compliance with the certification in case of grave data breach incidents relating to the scope of the certification and the ToE. The Board understands by this requirement that in case that a significant data breach, related with the scope of the certification and the ToE, occurs, which indicates, by its nature, that the client had not taken appropriate measures as expected according to its certification, in the sense that , if the relevant certification requirements were indeed properly implemented, such a data breach would not have been occurred, then this should be considered as non-compliance with the certification, and appropriate actions should be taken by the certification body. The Board encourages the CY SA to clarify in its accreditation requirement.

1.2.6 MANAGEMENT SYSTEM REQUIREMENTS

24. With respect to section 8 of the CY SA's draft accreditation requirements, the CY SA refers to the Guidelines "These management principles and their documented implementation must be transparent and be disclosed by the accredited certification body pursuant in the accreditation procedure pursuant to Article 58 and at the request of the Office of CPDP at any time during an investigation in the form of data protection reviews pursuant to Art. 58(1)(b) of the GDPR or a review of the certifications issued in accordance with Article 42(7) of the GDPR pursuant to Article 58(1)(c) of the GDPR". The Board notes that the part of the sentence stating that "the accredited certification body pursuant in the accreditation procedure pursuant to Article 58" is reflected in the Guidelines, but this requirement, as stands, creates confusion. To this purpose, the Board recommends the CY SA to delete this part of the sentence.

2 CONCLUSIONS / RECOMMENDATIONS

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

26. Regarding 'resource requirements', the Board recommends that the CY SA:

    1) amend the requirement in section 6.1, by replacing the term "degree" with the term "qualification" in order to bring it line with the Guidelines.

    2) add in section 6.1, on top of the "relevant professional experience", that this experience must also be significant.

    3) replace in section 6.1 (bullet 3), the term "technical" procedures with the term "comparable".

27. Regarding 'management system requirements', the Board recommends that the CY SA:

    1) remove, in section 8, the part of the sentence stating that "the accredited certification body pursuant in the accreditation procedure pursuant to Article 58" so to avoid creating confusion.

3 FINAL REMARKS

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

29. According to Article 64 (7) and (8) GDPR, the CY 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.

30. The CY 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

(Anu Talus)