Opinion 37/2023 on the draft decision of the competent supervisory authority of Luxemburg regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)

Adopted on 21 December 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 Luxemburgish SA (hereinafter "LU SA") has submitted its draft accreditation requirements under Article 43 (1)(a) to the EDPB. The file was deemed complete on 26 October 2023. The LU SA will perform accreditation of certification bodies to certify using GDPR certification criteria.

2. This is the second set of accreditation requirements for certification bodies that the LU SA submits to the Board. Pursuant to LU SA's draft national decision, the first set of accreditation requirements submitted to the Board will only be applicable to certification bodies that wish to provide certification services in the context of the national certification scheme "GDPR-CARPA", approved by the LU SA on 13 May 2022[3] or any future certification scheme using the ISAE3000 standard as an audit methodology. On this first set of requirements, the Board issued an Art. 64 (c) Opinion (5/2020). This set of requirements were revised taking on board this EDPB Opinion, pursuant to Art. 10(8) of the EDPB RoP.

   The second set of accreditation requirements will be applicable to certification bodies that want to provide certification services in the context of all other certifications schemes that are not using the ISAE3000 standard as a required audit methodology. Thus, the Board provides a new Art. 64(c) Opinion on this new subject matter.

[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] Decision N° 15/2022 of the CNPD

2 ASSESSMENT

2.1 General reasoning of the EDPB regarding the submitted draft decision

3. 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 LU SA is tasked by national law to carry out the accreditation of certification bodies. To this end, the LU 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].

4. This assessment of LU 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.

5. 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.

6. 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.

7. 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 reproducing the text.

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

9. This opinion does not reflect upon items submitted by the LU 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.

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:

2.2.1 GENERAL REMARKS

11. The Board acknowledges that the LU SA makes reference to the “ISO/IEC 17065:2012” standard in the introductory part but also later on in the draft requirements (e.g. section 2 “normative reference”

section 2 “terms and definitions”). The Board encourages the LU SA to cite consistently this term throughout the accreditation requirements.

12. Similarly, the Board notices that the term “Target of Evaluation” is defined under section 3 of the LU SA’s accreditation requirements. However, in other parts of the requirements, such as in section 6.1.1.4 the LU SA refers to the “object of evaluation” instead of referring to the “Target of Evaluation”. For consistency purposes and in order to avoid confusion, the Board encourages the LU SA to use this term consistently in the entire text of the requirements.

13. With respect to section 3 on “terms and definitions”, the Board welcomes the fact that the LU SA defines the term accreditation requirements as “the requirements established by the competent supervisory authority against which an accreditation is performed and which are not based on EN-ISO/IEC 17065/2012”. Considering that these additional requirements are adding up to the GDPR ones, the Board encourages the LU SA to replace the term “which are based on” with “in addition to” so to more clearly reflect that these requirements are additional to the requirements stemming from the GDPR.

14. With respect to the definition of the Target of Evaluation, the Board encourages the LU SA to bring this definition in line with the Guidelines, by adding that the relevant processing operations can include the personal data processed, the technical systems used and the related processes and procedures.

15. For the sake of consistency and in order to avoid confusion, the Board encourages the LU SA to replace the term “an organisation the certification body certifies”, in section 4.2.6 of its draft requirements, and replace it with the term “client” as defined in the terms and definitions section of the requirements.

16. The Board notices that the LU SA, in the section 3 “terms and conditions” of the draft accreditation requirements, makes references, in addition to the definitions stemming from the Guidelines, to GDPR definitions, such as this of controller, processor and personal data. In order to limit the possibility of confusion and of interpretation of such definitions by the certification body, the Board encourages the LU SA to remove the text of the definitions and when referring to controllers, processors and other terms from the GDPR, instead refer to Article 4 of the GDPR and the respective provision instead.

2.2.2 GENERAL REQUIREMENTS FOR ACCREDITATION

17. In section 4.1.1.1 of its draft accreditation requirements, the LU SA provides that “The certification body shall be able to demonstrate to the CNPD its compliance to the present accreditation requirements as well as the GDPR in its capacities both, as certification body as well as data controller/processor”. The certification body shall be able to demonstrate evidence of GDPR compliant procedures and measures specifically for controlling and handling personal data in the context of the certification activities. The EDPB encourages the LU SA to modify this requirement accordingly.

18. The Board notes that in section 4.2.1 of the LU SA’s draft accreditation requirements on the management of impartiality, the LU SA states that the certification body shall provide separate evidence of its impartiality. The Guidelines refer to evidence of independence. The Board encourages the LU SA to modify this in accordance with the Guidelines.

19. In the same section of LU SA's draft accreditation requirements, the Board notices that the certification body shall establish and communicate policies and procedures. However, it is not clear from the draft requirements who will be the recipient of such policies and procedures. Thus, the Board encourages the LU SA to clarify in its draft requirements that such policies and procedures will be communicated, by making them available to the Supervisory Authority as well as to the relevant personnel, which will need to comply with them.

20. The Board takes note of the fact that the LU SA, in section 4.3.1.a of the draft requirements, states that the certification body, in addition to the requirements in p. 4.3.1 of ISO 17065, shall ensure on a regular basis that it has evaluated the risks related to its certification activities. However, for the Board it is not clear to which risks this evaluation refers. For clarity purposes, the Board encourages the LU SA to specify in the requirements that the risks referred to are financial risks.

21. In the same section of LU SA's draft accreditation requirements, letter b, the Board encourages the LU SA to add that appropriate measures are related not only to insurance, but also financial reserves, in accordance with the Guidelines.

22. In section 4.5.4 of its draft accreditation requirements, the LU SA states that "The certification body shall establish policies and procedures designed to maintain the confidentiality, safe custody, integrity, accessibility and retrievability of engagement documentation." In order to avoid confusion and for consistency purposes, the Board encourages the LU SA to either clarify that such terms have the same meaning as the terms "confidentiality, integrity and availability" or to replace the currently used terms with these ones, coming from the Guidelines.

23. With respect to the same section of the LU SA's draft accreditation requirements, the Board notes that there's the inclusion of the term "engagement documentation". The Board encourages the LU SA to either define this term in the terms and definitions section or to include a clearer term that would facilitate the certification body's understanding of this requirement.

2.2.3 PROCESS REQUIREMENTS

24. The Board notes that section 7.2.1 (b) of the LU SA's draft accreditation requirements ("application") contains a reference to the controller/processor contract(s) and their specific arrangements. While acknowledging that the LU SA has used the wording of the Annex, the Board encourages the LU SA to also include a reference to joint controllers and their specific arrangements, pursuant to Art. 26 of the GDPR.

3 CONCLUSIONS / RECOMMENDATIONS

25. The Board has assessed the draft accreditation requirements of the Luxemburgish Supervisory Authority and did not identify any issues which might lead to an inconsistent application of the accreditation of monitoring bodies.

4 FINAL REMARKS

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

27. According to Article 64 (7) and (8) GDPR, the LU 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.

28. The LU 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)