
# 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)

**Adopted on 29 January 2020**

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 Article 51 (1b) of Directive 2016/680 EU on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (hereafter "Law Enforcement Directive").

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.

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

(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 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 LU SA has submitted its draft accreditation requirements under Article 43 (1)(a) to the EDPB. Following a decision deeming the file complete, it was broadcasted on 25 October 2019. The LU SA will perform accreditation of certification bodies to certify using GDPR certification criteria.

2. In compliance with article 10 (2) of the Board Rules of Procedure, due to the complexity of the matter at hand, the Chair decided to extend the initial adoption period of eight weeks by a further six weeks.

# 2 ASSESSMENT

## 2.1 General reasoning of the EDPB regarding the submitted draft accreditation requirements

The purpose of this opinion is to assess the accreditation requirements developed by a SA, either in addition to ISO 17065 or as 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

[2] Para. 39 Guidelines: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_en.pdf

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 .

The assessment of the accreditation requirements is aimed at examining variations (additions or deletions) from the Guidelines and notably the Annex. Furthermore, the EDPB's Opinion is also focused on all aspects that may impact a consistent approach regarding the accreditation of certification bodies.

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.

The Board has conducted its assessment in line with the structure foreseen in Annex 1 to the Guidelines. When this Opinion remains silent on a specific section of the LU SA's draft accreditation requirements, it should be read as the Board is not having any comments and is not asking the LU SA to take further action. The Board notes that the LU SA has provided information to help the assessment of the draft accreditation requirements. However, the Opinion of the Board only addresses the draft accreditation requirements.

Furthermore, 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.

3. 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)

the Board is of the opinion that:

### 2.2.1 GENERAL REMARKS

4. The Board notes that the draft accreditation requirements do not completely follow the structure set out in Annex 1 to the Guidelines. For example, the sections on "scope" and "terms and definitions" are missing. In connection to this, the Board notes that some terms are not used consistently throughout the document, such as "client" and "applicant". In order to avoid confusion, the terms used should be aligned with the Guidelines and the Annex definitions where possible and used consistently. Therefore, with the aim to facilitate the assessment, the Board encourages the LU SA to follow the structure of Annex 1 [to the Guidelines] in the draft accreditation requirements and add the missing sections..

5. The Board observes that, throughout the document, there are several references to the requirements "of this certification mechanism" (for example requirement 4.6.4) or to certification bodies that are accredited "under the (...) certification mechanism" (for example requirement 2.2.2). The reference to the certification mechanism seems to be a drafting issue. Thus, the Board encourages the LU SA to redraft the references in order to reflect that the certification bodies are accredited against the requirements approved by the supervisory authority.

6. On a similar note, the reference to the "requirements set out in this certification mechanism", used throughout the document (for example requirement 1.1.1.2), is confusing. A more appropriate reference could be "the criteria set out in the certification mechanism". Thus, the Board encourages the LU SA to clarify all references to "the certification mechanism" throughout the document.

7. The Board observes that several requirements (e.g. 3.2.1.1 and 4.1.2) refer to the "relevant International Standards", the "relevant standard" or the "specified standard". However, there is no definition of such standards and, therefore, it is unclear which are the standards referred to. Thus, the Board recommends the LU SA to clarify the meaning of such standards. This could be done, for example, in the "scope" or "terms and definitions" sections.

### 2.2.2 GENERAL REQUIREMENTS FOR ACCREDITATION

8. The Board notes that LU SA requirement 1.1.1.1 refers to another standard ("ISAE 3000"), which the EDPB has not assessed. Therefore, the Board recommends the LU SA to clarify that the requirements cannot be overridden by any external standard, such as ISAE 3000.

9. The Board notes that the requirements in 1.6 do not include the obligation of the certification body to publish and make easily publicly available all versions of the approved criteria and all certification procedures, as established in the Annex to the Guidelines (section 4.6). The Board notes that LU SA

might be the certification scheme owner , however the Board considers that it would be helpful to add an appropriate reference to ensure that the criteria is up to date and easily accessible via the certification body itself. In this regard, the Board considers that by making the information available only upon request, as set up in requirement 1.6.1, the LU SA is stablishing a stricter requirement than the Annex, which establishes that the information shall be make easily publicly available. Therefore, the Board recommends the LU SA to amend the requirement in order to include the obligation of the certification body to make easily publicly available all versions of the approved criteria and all certification procedures, in line with the Annex to the Guidelines.

10. The Board notes that requirement 1.2.4 refers to the 'certified process'. The Board considers that more precise wording, in line with the Guidelines could be used, such as 'certified processing operations/activities'. This provides for the broader certification scope, as provided by GDPR. Therefore, the Board encourages de LU SA to amend the draft requirements accordingly.

### 2.2.3 RESOURCE REQUIREMENTS

11. The Board notes that requirement 3.1.1.2 seems repetitive and unclear, not helped by the different terminology. For example, the third paragraph reads as if the engagement partner makes the decision of suitability on their judgement alone. The Board recommends LU SA to redraft to make the requirement clearer and more understandable, using consistent terminology.

### 2.2.4 PROCESS REQUIREMENTS

12. The Board observes that requirement 4.2.1 provides several examples of necessary information. Nonetheless, the first two examples provided should be a requirement by themselves, in accordance with section 7.2 of the Annex 1 to the Guidelines. Therefore, the Board encourages the LU SA to amend the wording and include the above-mentioned examples as requirements.

13. With regard to section 4.4 (Evaluation) of the LU SA accreditation requirements, the Board is of the opinion that the accreditation requirements should include the obligation of the certification body to ensure that there are evaluation methods in place, and that those evaluation methods, described in the certification mechanism, are standardised and generally applicable. This would ensure that comparable evaluation methods are used for comparable targets of evaluation. Any deviations from these evaluation methods would need to be justified by the certification body. Hence, the Board recommends the LU SA to amend the draft in order to include the above-mentioned obligation for the certification body.

14. Furthermore, the Board takes note that requirement 4.4.2 states that, even though outsourcing is not allowed, the certification body can use external experts for specific areas. In this regard, it is important to clarify that the certification body will retain the responsibility for the decision-making, even when it uses external experts. Therefore, the Board recommends the LU SA to amend the wording in requirement 4.4.2 accordingly.

15. The Board observes that section 4.7 of the LU SA accreditation requirements ("certification documentation") does not address the requirement in the Annex for documenting the period of surveillance (section 7.9). Therefore, the Board encourages the LU SA to include the period of monitoring within the meaning of section 7.9 on surveillance.

16. With regard to section 4.8 ("directory of certified processing activities") of the LU SA accreditation requirements, requirement 4.8.1 states that the information will be provided to the public "upon request". The Board is of the opinion that, the transparency obligation set out in section 7.8 of Annex

1 would be better fulfilled if the information was made available pro-actively by the certification body. Thus, the Board recommends the LU SA to amend the draft in order to provide that the certification body will make publicly available the information referred to in section 7.8 of Annex 1 of the Guidelines.

17. The Board notes that section 4.8 has a heading for surveillance without any requirements. The Board recommends that LU SA to clarify how monitoring will be carried out.

18. Concerning the termination, reduction, suspension or withdrawal of certification (subsection 4.10), the Board notes that there is no reference to the obligation of the certification body to accept decisions and orders from the competent supervisory authority to withdraw or not to issue certification to a customer (applicant) if the requirements for certification are not or no longer met. This obligation is set out in Article 58(2)(h) GDPR as well as in section 7.11 of Annex 1. Therefore, the Board recommends the LU SA to amend the accreditation requirements specifying the rules covering withdrawal, termination, reduction or suspension of the certification .

19. The Board notes that section 9 of the annex which has general headings do not have requirements. For example, section 9.3.4 on suspension or withdrawal of accreditation in not covered here. These are significant headings that warrant cross references to the relevant sections or requirements being added. The Board encourages LU SA to clarify where the requirements are covered.

# 3 CONCLUSIONS / RECOMMENDATIONS

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

21. As general remarks, the Board recommends that the LU SA:

    1. clarifies the meaning of “standard”, as referred in several requirements (e.g. 3.2.1.1 and 4.1.2). This could be done, for example, in the “scope” or “terms and definitions” sections.

22. Regarding ‘general requirements for accreditation’ the Board recommends that the LU SA:

    1. clarifies that the requirements cannot be overridden by any external standard, such as ISAE 3000.

    2. amends the requirements in 1.6 in order to include the obligation of the certification body to publish and make easily publicly available all versions of the approved criteria and all certification procedures, in line with the Annex to the Guidelines.

23. Regarding ‘resource requirements’ the Board recommends that the LU SA:

    1. redrafts requirement 3.1.1.2 to make it clearer and more understandable, using consistent terminology.

24. Regarding ‘process requirements’ the Board recommends that the LU SA:

    1. amends section 4.4 of the draft requirements in order to include the obligation of the certification body to ensure that there are evaluation methods in place, and that those

evaluation methods, described in the certification mechanism, are standardised and generally applicable. Any deviations from the evaluation methods would need to be justified by the certification body.

2. amends the wording in requirement 4.4.2 in order to make explicit that the certification body will retain the responsibility for the decision-making, even when it uses external experts.

3. amends section 4.8 of its draft accreditation requirements in order to provide that the certification body will make publicly available the information referred to in section 7.8 of Annex 1 of the Guidelines.

4. clarifies in section 4.8 how the monitoring will be carried out..

5. amends subsection 4.10 in order to specify rules covering withdrawal, termination, reduction or suspension of the certification.

# 4 FINAL REMARKS

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

26. According to Article 64 (7) and (8) GDPR, the supervisory authority 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.

For the European Data Protection Board

The Chair

(Andrea Jelinek)