

# Opinion of the Board (Art. 64)



**Opinion 23/2020 on the draft decision of the competent supervisory authority of Italy 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	TERMS AND DEFINITIONS .....	6
2.2.2	GENERAL REQUIREMENTS FOR ACCREDITATION (Section 4 of the draft accreditation requirements).....	6
2.2.3	RESOURCE REQUIREMENTS (Section 6 of the draft accreditation requirements) .....	7
2.2.4	PROCESS REQUIREMENTS (Section 7 of the draft accreditation requirements) .....	7
2.2.5	MANAGEMENT SYSTEM REQUIREMENTS (section 8 of the draft accreditation requirements).....	7
3	Conclusions / Recommendations.....	8
4	Final Remarks .....	8

## 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,<sup>1</sup>

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

---

<sup>1</sup> 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.<sup>2</sup>

(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 Italian Supervisory Authority (hereinafter “IT SA”) has submitted its draft accreditation requirements under Article 43 (1)(b) to the EDPB. The file was deemed complete on 27 May 2020. The Italian 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 IT SA, once they are approved by the IT 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 IT 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.

---

<sup>2</sup> 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](https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_en)

3. This assessment of IT 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 IT SA's draft accreditation requirements, it should be read as the Board not having any comments and not asking the IT SA to take further action.
8. This opinion does not reflect upon items submitted by the IT 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 TERMS AND DEFINITIONS

10. The Board notes that, in '3 Terms and definitions', the IT SA defines 'Client' as "the data controller or data processor applying for certification". This deviates from ISO 17065, which states that whenever the term "client" is used, it applies to both the "applicant" (seeking certification) and the "client" (that has been certified). It also deviates from Annex 1 the guidelines on accreditation, which differentiates between "applicant" and "client". The Board encourages the IT SA to delete the definition of "client", and to either use the terms "applicant" and "client" as they are used in Annex 1 of the guidelines on accreditation or to use "client" as it is used in ISO 17065. If the IT SA chooses to do the latter, the Board encourages the IT SA to add a note that "client" is being used in this manner.

### 2.2.2 GENERAL REQUIREMENTS FOR ACCREDITATION (Section 4 of the draft accreditation requirements)

11. With regard to clause 7 of subsection 4.1.2 of the IT SA's draft accreditation requirements, the Board considers that the wording is slightly unclear with regard to whom the reasons for approving certification are provided. Therefore, the Board encourages the IT SA to redraft it in a way that provides more clarity.
12. With regard to subsection 4.3, the Board notes that the draft additional accreditation requirements require the certification body to "confirm [...] it complies with the payment of pension contributions and other allowances; it is not the subject of tax injunction orders [...]". The Board encourages the IT SA to clarify why these obligations, which are unrelated to the GDPR, are included in the draft additional accreditation requirements.

### 2.2.3 RESOURCE REQUIREMENTS (Section 6 of the draft accreditation requirements)

13. The Board notes that, in subsection 6.1, the draft additional accreditation requirements of the IT SA mostly follows the wording given in Annex 1 of the guidelines on accreditation. However, where Annex 1 states that certification personnel shall be “registered as applicable” this is omitted in the IT draft additional requirements. The Board recommends that the IT SA either reinstates the wording about certification personnel being “registered as applicable”, or clarifies that there is no obligation for registration under IT law.
14. The Board notes that in subsection 6.1, among the eligibility requirements for personnel responsible for certification decisions, it is stated that they “shall not be or have been struck off the respective professional registers on account of disciplinary reasons or any other grounds”. The Board encourages the IT encourages the IT SA to clarify why having been struck off the professional register on other grounds than disciplinary actions would lead to ineligibility.
15. The Board notes that, among the eligibility requirements for personnel responsible for certification decisions, it is stated that they “shall not be or have been the subject of measures restricting personal freedom”. The Board encourages the IT SA to clarify what is meant by “measures restricting personal freedom”.

### 2.2.4 PROCESS REQUIREMENTS (Section 7 of the draft accreditation requirements)

16. With regard to subsection 7.4 of the draft additional accreditation requirements, the Board encourages the IT SA to clarify the paragraph on pre-existing certification by replacing “previous certification activity” by “existing certification” and by clarifying what is meant by “the object of the latter”.
17. In the paragraph starting with “in addition to item 7.4.6 of ISO 17065”, the Board notes the wording “the CB shall set out in detail in its certification process...”. The Board encourages the IT SA to add that the CB shall set this out in a written document which could be either the certification scheme or, if the CB isn’t the scheme owner, another document pertaining to the certification process.
18. With regard to subsection 7.10 of the IT SA’s additional accreditation requirements, the Board considers that changes in the state of art are relevant and might affect certification. Therefore, the Board encourages the IT SA to include this possibility among the list of changes that might affect certification.

### 2.2.5 MANAGEMENT SYSTEM REQUIREMENTS (section 8 of the draft accreditation requirements)

19. In Annex 1 of the guidelines on accreditation, chapter 8 starts with subsection “8.1 General management system requirements”. In ISO 17065, chapter 8 starts with subsection “8.1 Options”. In their draft requirements, the IT SA also uses “8.1 Options”. To maintain the consistency with Annex 1, and in order to avoid misinterpretation by providing a clear and unambiguous reference to ISO 17065, the Board encourages the IT SA to change the title of subsection 8.1 to “8.1 General management system requirements”, and to refer to subsection 8.1 in ISO 17065 by its full title, i.e. “No additional requirements are laid down to 8.1 Options of ISO/IEC 17065:2012”.

### 3 CONCLUSIONS / RECOMMENDATIONS

20. The draft accreditation requirements of the IT Supervisory Authority may lead to an inconsistent application of the accreditation of certification bodies and the following changes need to be made:
21. Regarding 'resource requirements', the Board recommends that the IT SA:
  - 1) either reinstates the wording from Annex 1 about certification personnel being 'registered as applicable', or clarifies that there is no obligation for registration under IT law.

### 4 FINAL REMARKS

22. This opinion is addressed to the Italian Supervisory Authority and will be made public pursuant to Article 64 (5)(b) GDPR.
23. According to Article 64 (7) and (8) GDPR, the IT 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.
24. The IT 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)