Opinion 12/2022 on the draft decision of the competent supervisory authority of France regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)

Adopted on 4 July 2022

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 French Supervisory Authority (hereinafter "FR SA") has submitted its draft accreditation requirements under Article 43 (1)(b) to the EDPB. The file was deemed complete on 29 March 2022. The FR 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 FR SA, once they are approved by the FR 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 FR 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.

3. This assessment of FR 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

[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

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

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

2.2.2 GENERAL REMARKS

11. Section 5 of the draft accreditation requirements mentions that the CB shall inform the NAB regarding any other binding decision that may constitute a non-conformity to the requirements of this document. The EDPB encourages the FR SA to redraft this requirement so to include explicitly the decisions of the competent judicial authorities that may affect the accreditation.

12. In general, the Board encourages the FR SA to ensure consistency of the wording throughout the text (e.g. translation problem in section 4.6 heading). Similarly in section 7(3)(3)(f), there is a new term introduced, this of “candidate” instead of applicant.

2.2.3 GENERAL REQUIREMENTS FOR ACCREDITATION

13. Regarding section 4.1 “legal responsibility”, the Board encourages the FR SA to explicitly refer to up-to-date procedures and measures.

14. With respect to section 4.1.2(2) letter b, states that “the methods to be applied by the certification body for the assessment of the target of evaluation, as defined in the requirements in §7.3(2) b) of

this document". In this regard, the Board, for the sake of clarity, encourages the FR SA to redraft this requirement and bring it in line with the Guidelines (section 7(3)(1) of the Annex), by explicitly referring to binding character of the evaluation methods.

15. Concerning section 4.1.2(2) letter c of FR SA's draft accreditation requirements, regarding the organisation and the procedures to be put in place by the certification body for complaint and appeal management, the Board encourages the FR SA to bring it line with the Guidelines (section 4.1(8)) by adding the reference to "additionally, lit. j, shall also contain explicit statements on the structure and the procedure for complaint management in accordance with Article. 43(2)(d);".

16. Regarding section 4.1.3(1), letter a of the draft accreditation requirements, the FR SA refers to "certification mechanism is clearly referenced, and, where applicable, the subset of the criteria applicable to the target of evaluation is indicated". The Board encourages the FR SA to further explain in the requirements the essence of this concept of the subset of the criteria.

17. Regarding section 4.2 "management of impartiality", the Board notes that the draft accreditation requirements make reference only to rules to prevent the conflict of interest. The Board acknowledges the importance to have requirements to ensure, firstly, that there are no conflicts of interest and, secondly in case conflicts of interest are identified, that the certification body manages them. Therefore, the Board encourages the FR SA, in addition to having rules preventing conflicts, there should be clear rules to manage identified conflicts of interest.

18. Regarding section 4.2(b) "it is not affiliated to the client's organization nor does it share the same holding than its client", the Board encourages the FR SA to clarify the wording, in order to reflect the independence of the certification body. For example, the FR 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.

19. According to the Guidelines (Annex, section 4.1.2.2 " the certification body shall demonstrate in addition to requirements of ISO/IEC 17065/2012 that its certification agreements: require the applicant to allow full transparency to the competent supervisory authority with respect to the certification procedure, including **contractually confidential matters** related to data protection compliance". The Board notes that the explicit reference to the "contractually confidential matters" is missing in section 4.5 "confidentiality" of the draft accreditation requirements, thus the Board recommends the FR SA to include explicitly the obligation of the certification body to provide access to the SA to **contractually confidential matters**.

20. With respect to section 4.5.b of the FR SA's draft accreditation requirements, the Board encourages the FR SA to slightly modify the wording "the information to be published by the CNIL in the registry of certifications" and add submitted to the CNIL instead.

2.2.4 RESOURCE REQUIREMENTS

21. Regarding section 6.1(1) letters b and c, the Board recommends the FR SA to bring these in line with the Guidelines and add appropriate and relevant knowledge instead of appropriate experience.

22. With respect to section 6.1(3) last paragraph of the draft accreditation requirements, the latter make a reference to the scenario "when the personnel responsible for certification decisions does not have such knowledge and experience in personal data protection [...]". The Board understands that this refers to solely one decision that needs to be taken and for which the personnel lacks experience and

knowledge, but this does not in any way refer to the decision-making of the certification body as a whole. To avoid any confusion, the Board recommends that the FR SA further explains this in the requirements.

23. Similarly, in section 6.1(4) the Board recommends the FR SA to clarify what "Such expertise is not necessarily concentrated by one single individual. For instance it can be shared among the members of an evaluation team".

24. Section 6.2 "resources for evaluation" the Board recommends the FR SA to clarify that the certification body will retain the responsibility for the decision-making even when it uses external experts/bodies.

2.2.5 PROCESS REQUIREMENTS

25. With regards to section 7.2(1) letter h, the Board encourages the FR SA to clarify which information on recent sanction decisions and/or corrective measures imposed by the CNIL or other supervisory authorities to the applicant shall be obtained by the certification body. More precisely, the notion of "recent" needs elaboration. The same also applies for the Section 7.3(2) letter b.

26. With respect to section 7.2(1) letter h, the Board notes the reference to "information related to ongoing investigations, or recent sanction decisions and/or corrective measures imposed by CNIL or other supervisory authorities". However, for clarity purposes, the Board encourages the FR SA to clearly state that these are authorities, refer to competent authorities.

27. Regarding Section 7.4(2) letter b of the draft accreditation requirements "a method for evaluating the coverage, the type and assessment of all risks considered by the controller and the processor with regard to their obligations pursuant to Articles 30, 32 and 35 and 36 of the GDPR, and with regard to the appropriateness of technical and organisational measures pursuant to Articles 24, 25 and 32 of the GDPR", the Board encourages the FR SA to bring this requirement in line with the Guidelines, by adding "insofar as the aforementioned Articles apply to the object of certification".

28. With respect to section 7.4(3) of the FR SA's draft accreditation requirements, where it is mentioned that "where the certification body assigns to the evaluation tasks personnel that does not meet the "technical profile" nor the "legal profile" requirements (as defined in para. 6 of the requirements), it shall justify the need for assigning an "expert" with specific competencies for the need of the evaluation". The Board understands that this will in case in exceptional circumstances, where there will be a need for specific expertise, which the certification body's personnel will not have. However, the Board encourages the FR SA to appropriately rephrase this requirement so to avoid confusion.

29. As regards to section 7(5)(1) of the FR SA's draft accreditation requirements, the Board encourages the FR SA to clarify that the review of the process, as mentioned in section 7.5 of the Annex of the Guidelines, is to be conducted in line with section 7.9(2) of the draft certification requirements, where the regularity of the surveillance activities is required .

30. Regarding Section 7.8(1)(b) of the FR SA's accreditation requirements, the Board recommends that the FR SA amends this requirement so to ensure that, in line with the Guidelines, a meaningful description on the object of certification is in place.

31. With respect to the same section (note 1), where FR SA mentions that "this information does not have to be made public, contrary to the information detailed in section 7.8(2) of this document but shall be made available upon request to third parties that wish to make sure of the validity of a certification", the Board encourages the FR SA to clarify in the requirements why this distinction is made therein.

32. Regarding section 7.9(2) last paragraph of the FR SA's draft accreditation requirements, the Board encourages the FR SA to clarify that it will provide this information to CNIL in writing.

33. Concerning Section 7.10(2), the Board acknowledges that according to the FR SA's draft accreditation requirements, where there are changes affecting the certification process, the evaluation of the criteria shall be conducted, where required (see letter c in this section). However, the formulation in letter b may lead to misconceptions that such an immediate complementary evaluation or re-evaluation of the certification criteria will not be the case. Therefore, the Board encourages the FR SA to re-formulate this point to avoid any ambiguity by adding a first indent, requiring the documentation of an immediate complementary evaluation or re-evaluation of the certification criteria

2.2.6 MANAGEMENT SYSTEM REQUIREMENTS

34. Regarding section 8.1(1) of the FR SA's draft accreditation requirements, the Board recommends that the FR SA brings this section in line with the Guidelines, Annex, section 8, by ensuring to add the following to the requirements that the management system must specify a methodology for achieving and controlling these requirements in compliance with data protection regulations and for continuously checking them with the accredited body itself.

35. Regarding section to 8.1(2) the Board notes that to provide information must be disclosed at **any time**, and not only during the accreditation procedure, is missing. In particular, the accredited certification body must make public permanently and continuously which certifications were carried out on which basis (or certification mechanisms or schemes), how long the certifications are valid under which framework and conditions (recital 100). Therefore the Board recommends that the FR SA adds this to the accreditation requirements so to bring them in line with the Annex, section 8, of the Guidelines.

3 CONCLUSIONS / RECOMMENDATIONS

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

37. Regarding 'general requirements for accreditation', the Board recommends that the FR SA:

    1) includes in section 4.5 of the draft requirements an explicit reference to the obligation of the certification body to provide access to the SA to contractually confidential matters.

38. Regarding 'resource requirements', the Board recommends that the FR SA:

    1) redrafts the requirement of section 6.1.(1) letters b and c so to refer to appropriate and relevant knowledge instead of appropriate expertise.

    2) further explains in the section 6.1(3) last paragraph, that "when the personnel responsible for certification decisions does not have such knowledge and experience in personal data protection [...]", this refers to solely one decision that needs to be taken and for which the personnel lacks experience and knowledge, but this does not in any way refer to the decision-making of the certification body as a whole.

3) similarly, clarifies the reference to "such expertise is not necessarily concentrated by one single individual" in section 6.1(4) of the draft requirements.

4) clarifies in section 6.2 of the draft requirements that the certification body will retain the responsibility for the decision-making even when it uses externals/bodies.

39. Regarding 'process requirements', the Board recommends that the FR SA:

1) amends section 7.8(1)(b) of the draft requirements, to ensure, that in line with the Guidelines, a meaningful description on the object of certification is in place.

40. Regarding 'management system requirements', the Board recommends that the FR SA:

1) adds the following to the requirements that the management system must specify a methodology for achieving and controlling these requirements in compliance with data protection regulations and for continuously checking them with the accredited body itself.
2) includes that the information must be provided at any time.

4 FINAL REMARKS

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

42. According to Article 64 (7) and (8) GDPR, the FR 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.

43. The FR 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)