Opinion 12/2021 on the draft decision of the competent supervisory authority of Portugal regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)

Adopted on 23 March 2021

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 Portuguese supervisory authority (hereinafter "PT SA") has submitted its draft accreditation requirements under Article 43 (1)(b) to the EDPB. The file was deemed complete on 26 January 2021. The PT 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 PT SA, once they are approved by the PT 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 PT 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 PT 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 PT SA's draft accreditation requirements, it should be read as the Board not having any comments and not asking the PT SA to take further action.

8. This opinion does not reflect upon items submitted by the PT 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. The Board notes that the section on "scope" in the PT SA's draft accreditation requirements does not include the relevant elements of the Annex. In particular, it should be clear that GDPR certification is only applicable to processing operations and controllers and processors. The EDPB thus encourages the PT SA to include such clarification.

12. In addition, the Board notes that the use of the terms "client" and "applicant" are not clear in the text, especially considering that the definition under the Annex and under ISO 17065 varies. In addition, some terms such as "subject matter of the certification, ToE, object of evaluation, evaluation object" are used indistinctly in the draft requirements. Thus, the Board encourages the PT SA to clarify these terms and to ensure that clear and consistent wording is used thorough the document.

2.2.3 GENERAL REQUIREMENTS FOR ACCREDITATION

13. Concerning section 4.1.1 of the PT SA's draft accreditation requirements (Legal responsibility), the Board considers that the obligation of certification bodies to have up to date procedures that demonstrate compliance with the legal responsibilities set out in the terms of accreditation should be

explicitly included in the accreditation requirements. Moreover, the certification body shall be able to demonstrate evidence of GDPR compliant procedures and measures specifically for controlling and handling client organisation's personal data as part of the certification process. Therefore, the Board recommends the PT SA to amend the draft requirements accordingly.

14. With regard to the certification agreement (section 4.1.2), the Board notes that the first point does not include the obligation of the client to also comply with the general certification requirements within the meaning of 4.1.2.2 lit. a ISO 17065, as stated in the Annex. The Board encourages the PT SA to include such reference.

15. Regarding the obligation to allow full transparency to the PT SA with respect to the certification procedure (point 2), it should be clear that the information to which the PT SA has access includes contractually confidential matters related to data protection compliance. The EDPB recommends that the draft requirements are amended accordingly.

16. With regard to point 6, the Board notes that the reference to the deadlines and procedures is limited to those "resulting from the certification mechanism", whereas section 4.1.2, 5th indent of the Annex refers to deadlines in a broader manner by referring to the certification program *or other regulations*. Thus, the EDPB encourages the PT SA to amend the wording in order to refer to deadlines in a general manner, in line with the Annex.

17. With regard to point 7, the Board is of the view that the obligation to include in the certification agreement the rules setting appropriate intervals for re-evaluation or review should be explicitly mentioned. Thus, the Board recommend that the draft requirements be amended accordingly.

18. With regard to point 10, the Board notes that the PT SA's draft accreditation requirements include the obligation to "Explain the consequences of withdrawal or suspension of accreditation for the certification body, including how this impacts on the client". In this regard, section 4.1.2 par. 9 of the Annex establishes that the consequences for the customer in those cases shall be addressed. The Board understands that the intention of the PT SA is to ensure that the client is aware of the consequences in those situations and of the potential options or actions that can be taken. However, the Board considers that, in order to ensure that certification agreements accurately reflect not only the consequences and impact on the clients, but also the potential further actions, the PT SA's accreditation requirements should make clear that a simple explanation without addressing the potential next steps won't be sufficient. Thus, the EDPB encourages the PT SA to make clear that the customer should be aware of the consequences, the impact they have on them and the potential next steps that may be taken.

19. Additionally, the Board is of the opinion that point 11 of section 4.1.2 of the PT SA's draft accreditation requirements, regarding the obligation of the applicant to inform the certification body of infringements of the GDPR and of other data protection legislation, should be clarified. The Board considers that this obligation should not lead to self-incrimination and, therefore, the obligation should refer to infringements established by the PT SA and/or judicial authorities. Thus, the Board recommends the PT SA make such clarification. Moreover, in order to avoid confusion, the Board encourages the PT SA to clarify that "infringements" refer to infringements of the GDPR or other data protection certification that may affect certification.

20. With regard to section 4.2 of the PT SA's draft accreditation requirements (management of impartiality), the Board notes that the first paragraph states that "The certification body shall demonstrate *its independence in relation to the subject-matter of the certification* to the satisfaction

of the CNPD, in accordance to what is required in Article 43(2)(a) of the GDPR." The same wording is found in sections 6.1 and 6.2 of the PT SA's draft accreditation requirements. The EPDB understands that the intention is to refer to independence "towards the organisation under assessment" and encourages the PT SA to amend the draft accordingly.

21. In addition, the Board notes the obligation to lay down rules preventing conflicts of interest. The Board acknowledges the importance to have requirements that ensure, firstly, that there are no conflicts of interests and, secondly, in case conflicts of interest are identified, that the certification body manages them. Therefore, the Board encourages the PT SA to clarify that, in addition to having rules preventing conflicts, there should be clear rules to manage identified conflicts of interests.

22. With regard to the publicly available information (section 4.6 of the PT SA's draft accreditation requirements), the Board notes that point 1 refers to the publication of « all versions (either in force or not) of the certification criteria ». The Board encourages the PT SA to use a more accurate wording, by replacing "either in force or not" with "current and previous".

23. In addition, section 4.6 does not include the obligation to publish all certification procedures, generally stating the respective period of validity, as indicated in section 4.6 first indent of the Annex. Thus, the Board recommends that the draft accreditation requirements be amended accordingly.

2.2.4 RESOURCE REQUIREMENTS

24. With regard to the resource requirements, the EDPB considers that the draft accreditation requirements should be better aligned with the Annex. In particular, the elements listed under the first paragraph of section 6.1 Annex should be included. In this regard, only point 3 and, partially, point 2 seem to be covered in the draft requirements. In addition, the differences in the requirements for technical and legal personnel, and for evaluators and decision-makers are not clear. In fact, the Board notes that section 6.1 of the draft requirements do not seem to contain any requirements for technical personnel, whereas section 6.2 contains requirements for both legal and technical personnel carrying out evaluations. The Annex contains several requirements for technical and legal personnel carrying out evaluations and in charge of the decision-making. This difference is relevant, since the expertise and experience required varies between legal and technical personnel and also between those in charge of evaluations and decision-making. Taking into account that the requirements of the Annex need to be included in the draft requirements, the Board takes the opportunity to make the following remarks, in order to ensure that the inclusion of the requirements is done in a consistent manner: 1) regarding the educational requirements for personnel with technical expertise, the reference to a recognised protected title in the relevant regulated profession should be included; 2) legal personnel should have legal studies at a EU or state-recognised university for at least eight semesters. Thus, the EDPB recommend the PT SA to redraft the requirements in order to clarify the above-mentioned elements, in line with the Annex.

25. Moreover, the Board considers that the expertise requirements for evaluators and decision-makers should be tailored taking into account the different tasks that they perform. In this regard, the Board is of the opinion that evaluators should have a more specialist expertise and professional experience in technical procedures (e.g. audits and certifications), whereas decision-makers should have a more general and comprehensive expertise and professional experience in data protection. Considering this, the Board encourages the PT SA to redraft the requirements taking into account the different

substantive knowledge and/or experience requirements for evaluators and decision-makers. With regard to the reference to the knowledge of decision-makers of the ISO 17065 and the additional accreditation requirements, the Board notes that the same requirement could be applicable to personnel in charge of evaluation, and encourages the PT SA to amend the draft accordingly.

26. With regard to section 6.2 of the draft accreditation requirements, the Board notes that the PT SA has included additional requirements. In this regard, it is important to ensure that the requirements under section 6.1 and 6.2 are not contradictory. Thus, the EDPB encourages the PT SA to take into account the additional requirements to be included under section 6.1 and adapt section 6.2 accordingly.

2.2.5 PROCESS REQUIREMENTS

27. With regard to the process requirements, section 7.1 of the PT SA's draft accreditation requirements states that "If the certification body intends to act in other Member States, it shall obtain the necessary approval from the relevant competent authorities, *or apply for a European Data Protection Seal in accordance with Article 42(5) of the GDPR.*" This sentence seems to give the choice to the certification body to either obtain the approval from the competent SAs or to apply for an EU Data Protection Seal. The Board underlines that, even when an EU Data Protection Seal has been approved, the certification body still has to notify the relevant CSAs before operating it in a new Member State from a satellite office. This is especially relevant, considering that accreditation of a certification body granting European Data Protection Seals may have to be carried out in each of the Members States where the certification body is established.[3] However, it shall be noted that the CSAs should be notified even in those cases in which the operation of an EU Data Protection Seal in a new Member State does not require a new accreditation. Therefore, the Board recommends the PT SA to include the above-mentioned reference. For example, the draft requirements could state the following (see proposed amendments in italics): "If the certification body intends to act in other Member States, it shall *notify and, when necessary,* obtain the necessary approval from the relevant competent authorities, *including for the operation of a European Data Protection Seal in accordance with Article 42(5) of the GDPR*".

28. Concerning paragraph 4 of section 7.1 of the PT SA's draft accreditation requirements, the Board takes note of the additional requirement whereby a certification body shall investigate the client "for breaches of the data protection legal regime when it is notified by the client that it is being the subject to an inquiry carried out by the CNPD or if the supervisory authority so informs the certification body". It should be clear that such investigation should be linked with the scope of certification and the target of evaluation. Therefore, the Board recommends that the PT SA amend its requirement accordingly, by specifying that the investigation should be linked with the scope of certification and the target of evaluation.

29. The Board notes that point 2 of section 7.2 of the PT SA's draft accreditation requirements ("application") contains a reference to the controller/processor contract(s) and their specific arrangements. While acknowledging that the PT SA has used the wording of the Annex, the Board encourages the PT SA to include a reference to joint controllers and their specific arrangements.

30. In addition, the Board notes that point 3 of section 7.2 of the PT SA's draft accreditation requirements includes the obligation to identify "Any investigation or inquiry carried out by the CNPD to the

[3] In this regard, see Guidelines 1/2018, paragraph 44.

applicant, current or occurred since 25 May 2018". The Board is of the opinion that the obligation should be tailored to investigations or regulatory actions related to the scope of the certification and the target of evaluation. Therefore, the Board encourages the PT SA to clarify that the investigation or regulatory action should be related to the scope of certification and the target of evaluation.

31. With regard to section 7.4 of the PT SA's draft accreditation requirements ("evaluation"), the Board notes that the requirements state that "The certification body shall take into account the EDPB guidelines in what concerns the evaluation procedure, ensuring the homogeneity and consistency of evaluation methods for similar evaluation objects". Firstly, the Board considers that the reference to the EDPB Guidelines may limit the obligation of the certification body, in the sense that it only requires to take into account the EDPB guidelines regarding the evaluation procedure. Thus, the reference should be deleted or amended in a way that it avoids such limitation. Secondly, the Board notes that the Annex refers to evaluation methods that are "standardized and generally applicable. This means that comparable evaluation methods are used for comparable ToEs." The Board considers that the wording of the PT SA's draft accreditation requirements do not fully reflect the intention of the Annex to ensure the standardization of evaluation methods and, therefore, they should be amended accordingly. Thus, the EDPB encourages the PT SA to make the necessary changes mentioned above.

32. In addition, the EDPB recommend the PT SA to include the obligation of the CB to justify any deviation from the procedure referred in the previous paragraph, in line with the Annex.

33. With regard to paragraph 1, indent 3th of section 7.4, the Board notes that the PT SA's draft accreditation requirements do not mention the guarantees as one of the elements to be included in the method for assessing the remedies, as stated in the Annex. In addition, the Board notes that paragraph 1, indent 3th of section 7.4 of the Annex refers to demonstrating compliance with the legal requirements set out in the criteria. This reference is missing in the PT SA's draft accreditation requirements. Hence, the Board encourages the PT SA to include the above-mentioned references, in line with the Annex.

34. With regard to the use of certifications previously obtained, the Board notes that the PT SA's draft accreditation requirements mention a certification that the client wishes to "transfer". The same wording is found in section 7.9. The EDPB understands that the sentence refers to previous certifications that the client wishes to use. Thus, in order to avoid any confusion, the EDPB encourages the PT SA to clarify the meaning of "transfer". In addition, the Board considers that, when existing certification is taken into account as part of a new evaluation, it should be clear that it will not be sufficient to completely replace (partial) evaluations and that the scope of said certification should be assessed in detail in respect of its compliance with the relevant certification criteria. Besides, a complete evaluation report or information enabling an evaluation should be available to the certification body. The Board recommends the PT SA to amend the draft accordingly.

35. Furthermore, the Board notes that the use of external experts contracted by the certification body is foreseen in the PT SA's draft accreditation requirements. The Board considers that the draft accreditation requirements should explicitly state that the certification body will retain the responsibility for the decision-making, even when it uses external experts. Therefore, the Board recommends the PT SA to amend the draft accordingly.

36. The EDPB understands that paragraph 8 of section 7.4 refers to follow-up assessments of clients already certified. In order to avoid misunderstanding, the EDPB encourages the PT SA to make it clear in the text.

37. The Board notes that the second paragraph of section 7.6 of the PT SA's draft accreditation requirements ("certification decision") includes the obligation to submit to the PT SA the draft certification of conformity of documentation replacing it, prior to issuing or renewing certification. Based on the explanations provided by the PT SA, the Board understands that the intention of this requirement is to increase transparency and it does not entail a supervision of the draft approval. The Board encourages the PT SA to include a clarification in that sense.

38. With regard to section 7.9 of the PT SA's draft accreditation requirements ("Surveillance"), the Board welcomes the obligation to carry out the surveillance activities annually. In addition, the Board considers that the risks associated with the processing should be taken into account in order to determine whether a more frequent monitoring is necessary. Thus, the Board encourages the PT SA to include a risk-based approach in order to identify whether, in specific cases, the surveillance activities have to be carried out more than once per year.

39. With regard to section 7.10 of the PT SA's draft accreditation requirements ("changes affecting certification"), the Board considers that changes in the state of art are also relevant and might affect certification. Therefore, the Board encourages the PT SA to include this possibility among the list of changes that might affect certification.

40. In addition, the Board notes that point 1 under section 7.10 includes "any personal data breach notification or non-compliance of the GDPR or of the additional requirements". The Board considers that, in order to avoid self-incrimination, the reference should be to infringements established by the PT SA or the competent judicial authority. Additionally, the reference to "any data breach notification" seems quite broad. The Board is of the view that such reference should be tailored to data breach notifications that may be related to the scope of the certification and the target of evaluation. Therefore, the Board encourages the PT SA to add the abovementioned reference.

41. Regarding the fourth bullet point ("relevant decisions of the European Data Protection Board") the Board acknowledges that the PT SA has used the wording foreseen in Annex 1. However, in order to ensure a clear understanding of what is meant by "decisions of the European Data Protection Board", the Board encourages the PT SA to clarify the reference. An example could be to refer to "documents adopted by the European Data Protection Board".

42. With regard to section 7.11 of the PT SA's draft accreditation requirements ("Termination, reduction, suspension or withdrawal of certification"), the Board notes that the NAB should also be informed about the termination, reduction, suspension or withdrawal of certification. Therefore, the EDPB recommends that such reference be included.

43. The Board observes that section 7.11 of the PT SA's draft requirements (termination, restriction, suspension or withdrawal of certification) does not contain the obligation of the certification body to accept decisions and orders from the PT SA to withdraw or not to issue certification to an applicant if the requirements for certification are not or no longer met. Therefore, the Board recommends the PT SA to include such obligation.

44. With regard to section 7.13 of the PT SA's draft accreditation requirements ("complaints and appeals"), the EPDB notes that the following requirement from the Annex is missing: "(...) the certification body must define how separation between certification activities and the handling of appeals and complaints is ensured." The EDPB recommends the PT SA to amend the draft accordingly.

2.2.6 MANAGEMENT SYSTEM REQUIREMENTS

45. The Board notes that section 8 of the PT SA's draft accreditation requirements does not include the obligation to disclose to the PT SA the management principles and their documented implementation during the accreditation procedure and, afterwards, at the request of the PT SA at any time during an investigation, as stated in the Annex. The EDPB recommend that such obligation be included in the PT SA's accreditation requirements.

2.2.7 FURTHER ADDITIONAL REQUIREMENTS

46. Paragraph 5 of section 7.1 of the PT SA's draft accreditation requirements includes some of the elements of section 9.3.1 Annex ("communication between CB and its customers"). However, the EDPB notes that some elements from the Annex are still missing (e.g. references to maintaining documentation in order to enable contact in the event of a complaint and maintaining an application process for the purpose of or evaluations by the competent SA). The EDPB recommends the PT SA to include the missing elements from section 9.3.1 of the Annex.

47. Paragraph 3 of section 7.4 of the PT SA's draft accreditation requirements include the obligation of the certification body to periodically review its evaluation methods in light of the development of new technologies and changes in the legal framework. The Board notes that this requirement partially mirrors the requirement under section 9.1 of the Annex, since it seems to imply the existence of rules to review the evaluation methods. However, it should be clear that the certification body should establish procedures to guide the updating of evaluation methods. In addition, the update should take into account not only the development of new technologies and changes in the legal framework, but also the relevant risk(s), the state of the art and the implementation costs of technical and organisational measures, in line with the Annex. Thus, the Board encourages the PT SA to include the abovementioned elements.

48. Finally, the last sentence of section 7.13 of the PT SA's draft accreditation requirements partially reflect the obligation under second paragraph of section 9.3.3 of the Annex. However, the Board considers that relevant complaints and objections not only have to be informed to the PT SA, but they have to be shared with the PT SA. Therefore, the Board recommends the PT SA to redraft the requirement by stating that relevant complaints and objections shall be shared with the PT SA.

3 CONCLUSIONS / RECOMMENDATIONS

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

50. Regarding 'general requirements for accreditation', the Board recommends that the PT SA:

1) amend section 4.1.1 in line with the Annex
2) clarify in section 4.1.2, second point, that the information to which the PT SA has access includes contractually confidential matters related to data protection compliance.
3) add in section 4.1.2, point 7, the obligation to include in the certification agreement the rules setting appropriate intervals for re-evaluation or review.

4) clarify in section 4.1.2, point 11, that the obligation to inform about any infringements of the GDPR refers to infringements established by the PT SA and/or judicial authorities.

5) include in section 4.6 the obligation to publish all certification procedures, generally stating the respective period of validity.

51. Regarding 'resource requirements', the Board recommends that the PT SA:

1) clarify the requirements under section 6.1 in line with the remarks in paragraph 24 above.

52. Regarding 'process requirements', the Board recommends that the PT SA:

1) amend section 7.1 in order to include the references to the notification of the CSAs before the certification body operates in a new Member State from a satellite office, including for the operation of a European Data Protection Seal.

2) clarify in section 7.1 that the investigation that the certification body can carry out should be linked with the scope of certification and the target of evaluation.

3) include in section 7.4 the obligation of the CB to justify any deviation from the standardised and generally applicable evaluation methods.

4) include the elements mentioned in paragraph 34 of this Opinion, regarding the use of existing certification as part of a new evaluation.

5) explicitly state that the certification body will retain the responsibility for the decision-making, even when it uses external experts.

6) clarify that the NAB should also be informed about the termination, reduction, suspension or withdrawal of certification.

7) include the obligation of the certification body to accept decisions and orders from the PT SA to withdraw or not to issue certification to an applicant if the requirements for certification are not or no longer met.

8) amend section 7.13 to include the missing element from the Annex, as stated in paragraph 44 above.

53. Regarding 'management system requirements', the Board recommends that the PT SA:

1) include the obligation to disclose to the PT SA the management principles and their documented implementation during the accreditation procedure and, afterwards, at the request of the PT SA at any time during an investigation, as stated in the Annex.

54. Regarding 'further additional requirements', the Board recommends that the PT SA:

1) include the missing elements from section 9.3.1 Annex.

2) redraft the last sentence of section 7.13 by stating that relevant complaints and objections shall be shared with the PT SA.

4 FINAL REMARKS

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

56. According to Article 64 (7) and (8) GDPR, the PT 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.

57. The PT 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)