Opinion 38/2021 on the draft decision of the competent supervisory authority of Latvia regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)

Adopted on 20 November 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 Latvian SA (hereinafter "LV SA") has submitted its draft accreditation requirements under Article 43 (1)(b) to the EDPB. The file was deemed complete on 5 October 2021. The LV 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 LV SA, once they are approved by the LV 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 LV 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 the LV SA's additional accreditation requirements is aimed at examining on variations (additions or deletions) from the Guidelines and notably their Annex 1. Furthermore, the

[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

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

8. This opinion does not reflect upon items submitted by the LV 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 section “terms and definitions” states that definitions of the GDPR as interpreted in the relevant EDPB Guidelines take precedence over those of ISO/IEC 17065. The EDPB welcomes this clarification. However, some of the definitions in section “abbreviations” and in the draft itself do not correspond to the definitions used for the same concepts in the GDPR and the Guidelines. Thus, it is unclear what is the relationship between some of those terms and the definitions in the GDPR and Guidelines (e.g. definition of “accreditation”, reference to certification *program* instead of certification *criteria* in section 4.6.1.1). Therefore, the EDPB recommends the LV SA to ensure that the terms defined in the GDPR and/or the Guidelines are reflected consistently in the accreditation requirements.

12. The Board notes that the requirements should be drafted in a prescriptive manner. Thus, the requirements should avoid the word “should” and rather use “shall” or “must”. The EDPB encourages the LV SA to make the necessary changes in this regard (e.g. in sections 4.3.1 and 7.5.2).

13. The Board also notes that some of the terms used in the requirements should be clarified and clear and consistent wording should be used thorough the document (e.g. replace in section

"abbreviations", the reference to "accreditation plan" with "accreditation procedure"; replace "accreditation criteria" in section 7.1.2 with "certification criteria"; amend the reference to "full or partial compliance with the GDPR" in the definition of "subject of certification", since it may lead to misunderstandings -for example, the definition provided in paragraph 58 of the Guidelines could be used; replace "certification object" in section 7.8.2.1 with "subject of certification"; ensure a consistent use of terms in section 7.13 regarding the handling of complaints, instead of using different concepts with the same meaning, such as "examination of complaints", "review of complaints", "complaint handling";). The EDPB encourages the LV SA to amend the referred concepts and ensure that clear and consistent wording is used thorough the document.

14. In addition, the LV SA's draft requirements use the term "client" to identify both the applicant seeking certification and the certified entity. The Board encourages the LV SA to either use the terms "applicant" and "client" as they are used in Annex 1 of the guidelines on accreditation or to add a note that "client" is being used as identifying both applicant and certified entity.

15. Finally, the EDPB encourages the LV SA to add the specific reference to the EDPB Guidelines mentioned in the section "terms and definitions". This could be done, for example, by adding a footnote with the complete title and reference number of the guidelines.

2.2.3 GENERAL REQUIREMENTS FOR ACCREDITATION

16. Concerning section 4.1.1 of the LV 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 LV SA to amend the draft requirements accordingly.

17. With regard to section 4.1.1 ("Legal responsibility"), the Board is of the opinion that the certification body should confirm to the accreditation body not only that fact that they are not subject of any investigation or inspection by the LV SA, but also that they were not subject of such investigation/regulatory action in the past. Therefore, the Board encourages the LV SA to clarify this matter.

18. The EDPB notes that section 4.1.2.7 of the LV SA's draft requirements states: "that the Certification Body is allowed to disclose to the DSI all necessary information related to the reasons for granting the certification[3]". The Board underlines that such requirement should be read in line with the Annex, which requires to provide "all information necessary for granting certification" (see point 7 section 4.1.2 Annex).

19. 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 LV SA to include such reference.

[3]In conformity with Articles 43(5) and 42(8) of the GDPR.

20. The Board observes that the explicit reference to the tasks and powers of the competent SA (3rd indent in section 4.1.2 of the Annex) is not included in subsection 4.1.2.3 of the LV SAs' draft accreditation requirements. The Board is of the opinion that this reference should be added in the draft requirements and, therefore, it recommends the LV SAs to amend the draft accordingly.

21. Regarding section 4.1.2.6, the Board considers that it should specify that the certification agreement should contain the rules for validity, renewal and withdrawal, and the rules setting the intervals for re-evaluation or review, and recommends the LV SA to amend the draft accordingly.

22. In addition, section 4.1.2.9 states that the certification agreement will include the client's *obligation* to provide measures to review the complaints. However, according to the Annex, the certification agreement itself should include the *structure and the procedure* for complaint management as well as the necessary precautions for the investigation of complaints. Therefore, the EDPB recommends to amend the draft in order to include the above-mentioned references.

23. The Board notes that section 4.1.2.10 of the LV SA's draft accreditation requirements ("certification agreement") include the obligation to specify in the certification agreement "What are the consequences in case of revocation or suspension of the accreditation of the Certification Body, including the impact on the client and its certification". 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 LV 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 LV SA's accreditation requirements should make clear that simply listing the consequences without addressing the potential next steps won't be sufficient. Thus, the EDPB encourages the LV 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.

24. In addition, the Board notes that, according to the Annex, the applicant has to inform the certification body of significant changes in its actual or legal situation and in its products, processes and services concerned by the certification (10th indent in section 4.1.2 of the Annex). Section 4.1.2.11 of the LV SA's draft requirements refer to changes in the client's products, processes and services covered by the certification, without any mention to significant changes in its actual or legal situation". The Board encourages the LV SA to include a reference to significant changes in the client's actual or legal situation.

25. Additionally, the Board is of the opinion that section 4.1.2.11 of the LV 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 LV SA and/or judicial authorities. Thus, the Board recommends the LV SA make such clarification. Moreover, in order to avoid confusion, the Board encourages the LV SA to clarify that "infringements" refer to infringements of the GDPR or other data protection certification that may affect certification.

26. With regard to section 4.2 of the LV SA's draft accreditation requirements (management of impartiality), 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 LV SA to clarify that, in addition to having rules preventing conflicts, there should be clear rules to manage identified conflicts of interests.

27. In addition, the Board encourages the LV SA to provide examples of situations where a certification body has no relevant connection with the customer it assesses. For example, the certification body should not belong to the same company group nor should be controlled in any way by the customer it assesses.

28. Regarding section 4.6.1 ("Publicly available information"), the Board notes the obligation to make the information publicly available. In order to ensure transparency and easy access to such information, the Board recommends to clarify that the information should be made easily publicly available.

29. The Board also considers that, in section 4.6.1.3, the reference to publishing the period of validity of the certifications only "if possible" should be amended. Indeed, the Board is of the opinion that an indication of the general period of validity should be always possible. Thus, the Board encourages the LV SA to replace "if possible" by "generally".

2.2.4 RESOURCE REQUIREMENTS

30. With regard to the expertise of the certification body (section 6 of the LV SA's draft accreditation requirements), the Board considers that several of the general requirements of section 6.1 of the Annex are not covered. In particular, points 1, 2 with regard to ongoing expertise, 4, 5 and 6 are missing. Thus, the Board recommends the LV SA to amend the draft accordingly, so as to include the missing elements.

31. Regarding the specific requirements of personnel with technical and legal expertise, the Board notes that the distinction between the two types of personnel is unclear in the draft LV SA's accreditation requirements. Moreover, there isn't a clear difference between personnel in charge of certification decisions and personnel responsible for evaluations. The Board considers that, given the different tasks and responsibilities of the technical and legal personnel, as well as the personnel in charge of decision-making and personnel in charge of evaluations, a clearer distinction should be drawn with regard to the different type of education and experience required to the different types of personnel. Therefore, the EDPB recommends the LV SA to redraft the section clearly distinguishing the requirements applicable to legal personnel and to technical personnel, and to decision-makers and evaluators. If some of the requirements are applicable to both, it should be clearly stated as well. 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 LV SA to take into account the different substantive knowledge and/or experience requirements for evaluators and decision-makers.

32. Finally, the Board notes that the LV SA's draft requirements refer to the "Client's staff" (e.g. sections 6.1.1 and 6.1.2). The Board underlines that the accreditation requirements should focus on the requirements for the certification body's personnel and, therefore, recommends the LV SA to amend the draft, tailoring the requirements to the certification body's personnel and erasing any references to the client's personnel.

2.2.5 PROCESS REQUIREMENTS

33. Concerning section 7.1 of the LV SAs' draft accreditation requirements, the Board notes that there is no explicit reference to the obligation of the certification body to comply with the additional requirements. Even though such obligation could be inferred from the text of the draft requirements, the Board considers that an explicit reference to the above-mentioned obligation should be included. Therefore, the Board recommends the LV SAs to amend the draft accordingly.

34. With regard to sections 7.1.2.2 and 7.1.2.3, the Board understands, based on the explanations provided by the LV SA, that they refer to the approval of certification criteria in accordance with Art 42(5) GPDR. In order to avoid confusion as to the role of the LV SA in this regard, the EDPB encourages the LV SA to redraft the sections. For example, section 7.1.2.2 could state that the certification body "has received an approval decision regarding the certification criteria during the certification process, in accordance with Art. 42(5) GDPR" and section 7.1.2.3 could state "requests a new approval from the LV SA of the certification criteria when they are substantially changed".

35. Section 7.1.3 states that "*If the Certification Body intends to operate in other Member States, it shall obtain the necessary approval from the relevant supervisory authorities or apply for a European Data Protection Seal in accordance with Article 42(5) of the GDPR*." The EDPB notes that, even when operating an EU Data Protection Seal, the certification body has to notify the concerned SAs beforehand. The EDPB recommends that such clarification be added in the requirements.

36. Concerning section 7.1.4 of the LV SA's draft accreditation requirements, the Board takes note of the additional requirement whereby a certification body shall investigate the client "*for violations of the legal regime of personal data protection when the client declares that he/she is subject to an investigation by the LV SA or the LV SA informs the Certification Body about the investigation*". It should be clear that such investigation should be linked with the scope of certification and the target of evaluation. Additionally, it should be clear that the investigation refers to the certification holder and not to the applicant. Therefore, the Board recommends that the LV SA amend its requirement accordingly, by specifying that the investigation should be linked with the scope of certification and the target of evaluation and by clarifying that the investigation refers to the certification holder.

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

38. With regard to section 7.4.1.2, the Board notes that the LV SA's draft accreditation requirements include a reference to the assessment of the risks, but do not mention a method for evaluating the coverage and composition thereof. Hence, the Board encourages the LV SA to include the above-mentioned references, in line with the Annex.

39. Concerning section 7.4.1.4, the Board notes that the LV SA's draft requirements establish that the certification body shall demonstrate "*how it is ensured that comparable methods are used in evaluation and monitoring mechanisms, in comparable situations*". The Board considers that, for reasons of accuracy and clarity, the requirements should explicitly mention the obligation that the evaluations methods are standardized and generally applicable, and encourages the LV SA to make such addition.

40. In addition, the Board notes section 7.4.1.3 of the LV SA's draft accreditation requirements does not mention the guarantees and safeguards 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 4th of section 7.4 of the Annex refers to having a documentation of methods and findings. This reference is missing in the LV SA's draft accreditation requirements. Hence, the Board encourages the LV SA to include the above-mentioned references, in line with the Annex.

41. In addition, the EDPB recommends the LV 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.

42. Furthermore, the Board notes that the use of external experts contracted by the certification body is foreseen in the LV 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 LV SA to amend the draft accordingly.

43. In addition, the LV SA's draft accreditation requirements mistakenly refer to certification body as "the Client" or "the Tenderer" in sections 7.4.3, 7.4.4 and 7.4.5 regarding subcontractors. The Board understands that such references are due to a translation mishap. However, given the significance of the implications of referring to the client in those specific sections, the Board recommends that the references to "the client" be replaced by "the certification body" in section 7.4.3, 7.4.4 and 7.4.5 and that section 7.4.5 be amended in order to clarify the references to the client (for example, it could state "The *Certification Body* shall submit to the DSI a procedure specifying the significance of the compliance *of the client* with other certification [...]").

44. Regarding section 7.4.5.1.3 on the validity of the certification, the Board recommends the LV SA to clarify that the duration of validity of the GDPR certification must not be conditional upon the validity of other types of certifications.

45. Regarding section 7.4.8 of the LV SA's draft accreditation requirements, the Board considers that the LV SA's draft requirements should include the obligation of the certification body to set out in detail in its certification mechanism how the information required in item 7.4.6 ISO/IEC 17065/2012 shall be provided to the applicant about non conformities from a certification mechanism. Thus, the Board recommends the LV SA to include such obligation.

46. Regarding section 7.6.2 ("Certification decision"), the draft accreditation requirements include the obligation of the certification body to inform the LV SA prior to granting the certification. Based on the explanations provided by the LV SA, the Board understands that the intention is to increase transparency and it does not entail a supervision of the draft approval. The Board encourages the LV SA to include a clarification in that sense.

47. Section 7.6.3 establishes the obligation of the certification body to make sure, before taking a decision, that the LV SA has not initiated an investigation against the client. 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 LV SA to clarify that the investigation or regulatory action should be related to the scope of certification and the target of evaluation.

48. Section 7.7.2.1 ("Certification documents") states that the certificate should include *"the period of implementation of the planned monitoring measures".* In order to avoid confusion, the EDPB

encourages the LV SA to clarify that this includes the period of the intended monitoring, in accordance with the Annex.

49. The Board notes that section 7.8.2.1 ("Directory of certified products") states that the summary of the assessment report will include a "description" of the certified object. Such description should be meaningful, as specified in the Annex and, therefore, the EDPB recommends the LV SA to amend the requirements accordingly.

50. Furthermore, the obligation to inform about the reasons for granting or revoking certification is not only towards the LV SA but towards all concerned SAs. The EDPB recommends that section 7.8.3 be amended in order to include all the concerned SAs.

51. With regard to section 7.9.3 ("Surveillance") of the LV SA's draft accreditation requirements, 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 LV 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

52. With regard to section 7.10.1 of the LV 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 LV SA to include this possibility among the list of changes that might affect certification.

53. In addition, the Board notes that point 7.10.11 includes "any notification of personal data breaches, non-compliance with the requirements of the GDPR or these criteria". The Board considers that, in order to avoid self-incrimination, the reference should be to infringements established by the LV 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 LV SA to add the abovementioned reference.

54. Regarding the fourth bullet point ("relevant decisions of the EDPB") the Board acknowledges that the LV 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 EDPB", the Board encourages the LV SA to clarify the reference. An example could be to refer to "documents adopted by the EDPB".

55. With regard to section 7.11 of the LV SA's draft accreditation requirements ("Termination, reduction, suspension or withdrawal of certification"), the Board notes that there is no reference to informing about continuation of the certification. In addition, the NAB should also be informed about the continuation, termination, reduction, suspension or withdrawal of certification. Therefore, the EDPB recommends that such references be included. Moreover, the Board encourages the LV SA to clarify that the information should be provided in writing.

56. Concerning section 7.11.2, the Board underlines that the reference to investigations should be tailored to investigations related to the scope of the certification and the ToE. The Board encourages the LV SA to amend the draft accordingly.

57. The Board observes that section 7.11.3 refers to the LV SA not issuing certification or revoking it, if it considers that the certification criteria are not met or no longer followed. Based on the explanations provided by the LV SA, the Board understands that the intention is to it refer to the powers of the LV

SA to order the certification body not to issue or revoke certification if the certification criteria are not met or no longer met. The EDPB is of the view that, rather than restating the powers of the LV SA, the draft requirements should explicitly include the obligation of the certification body to accept decisions and orders from the LV 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 LV SA to include such obligation explicitly.

58. With regard to section 7.13.1.1 ("Complaints and appeals"), the Board underlines that the reference should not only be to complaints regarding the certification process but also to objections, in line with the Annex. The Board encourages the LV SA to add the reference.

59. In addition, the Board notes that section 7.13.1.3 establishes that the certification body shall determine "*who reviews the received complaints from the Certification Body, separating the persons who have made decisions on the issues for which the complaints have been received from the review of the complaints*". More in general and in accordance with the Annex, the certification body also needs to define how separation between certification activities and the handling of appeals and complaints is ensured. Thus, the Board recommends the LV SA to amend the draft accordingly.

60. Finally, the certification body should also define how and to whom the confirmation envisaged in item 7.13.2 of ISO/IEC 17065/2012 must be given. The Board recommends the LV SA to add such reference (e.g. in section 7.13.1.7).

2.2.6 MANAGEMENT SYSTEM REQUIREMENTS

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

62. In addition, the LV SA's draft accreditation requirements do not include the obligation to make public permanently and continuously "*how long the certifications are valid under which framework and conditions".* The Board acknowledges that section 4.6.1.5 of the LV SA's draft requirements refers to having a register of certified clients, including products, processes and services certified. The Board recommends to complete such section with the reference to the validity, framework and conditions of the certificate**.**

2.2.7 FURTHER ADDITIONAL REQUIREMENTS

63. The Board notes that the LV SA's draft accreditation requirements do not include any of the elements of section 9 of the Annex and recommends that such elements be included in the LV SA's accreditation requirements.

3 CONCLUSIONS / RECOMMENDATIONS

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

65. Regarding 'general remarks', the Board recommends that the LV SA:

1) ensure that the terms defined in the GDPR and/or the Guidelines are reflected consistently in the accreditation requirements.

66. Regarding 'general requirements for accreditation', the Board recommends that the LV SA:

1) amend section 4.1.1 in line with the remarks made in paragraph 16 of the present Opinion.

2) add in subsection 4.1.2.3 and explicit reference to the tasks and powers of the competent SA.

3) specify in section 4.1.2.6 that the certification agreement should contain the rules for validity, renewal and withdrawal, and the rules setting the intervals for re-evaluation or review.

4) add in section 4.1.2.9 that the certification agreement itself should include the *structure and the procedure* for complaint management as well as the necessary precautions for the investigation of complaints.

5) clarify in section 4.1.2.11 that the infringements are those established by the LV SA and/or judicial authorities.

6) clarify in section 4.6.1 that the information should be made easily publicly available.

67. Regarding 'resource requirements', the Board recommends that the LV SA:

1) add the missing elements of section 6.1 of the Annex, as explained in paragraph 30 above.

2) redraft section 6 clearly distinguishing the requirements applicable to legal personnel and to technical personnel, and to decision-makers and evaluators.

3) amend section 6, by tailoring the requirements to the certification body's personnel and erasing any references to the client's personnel.

68. Regarding 'process requirements', the Board recommends that the LV SA:

1) add in section 7.1 and explicit reference to the obligation of the certification body to comply with the additional requirements.

2) add in section 7.1.3 the clarification regarding the notification to the concerned SAs, as per paragraph 35 above.

3) amend section 7.1.4 by specifying that the investigation should be linked with the scope of certification and the target of evaluation and by clarifying that the investigation refers to the certification holder.

4) include the obligation of the CB to justify any deviation from the procedure referred to in paragraph 41 above.

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

6) replace the references to "the client" by "the certification body" in section 7.4.3, 7.4.4 and 7.4.5 and amend section 7.4.5 in order to clarify the references to the client.

7) clarify that the duration of validity of the GDPR certification must not be conditional upon the validity of other types of certifications.

8) include the obligation of the certification body to set out in detail in its certification mechanism how the information required in item 7.4.6 ISO/IEC 17065/2012 shall be provided to the applicant about non conformities from a certification mechanism.

9) amend the requirements in accordance with paragraphs 49 and 50 above.

10) amend section 7.11 in accordance with paragraph 55 above.

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

12) amend the requirements in accordance with paragraphs 59 and 60 above.

69. Regarding 'management system requirements', the Board recommends that the LV SA:

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

2) complete section 4.6.1.5 with the reference to the validity, framework and conditions of the certificate

70. Regarding 'further additional requirements', the Board recommends that the LV SA:

1) include the elements of section 9 of the Annex.

4 FINAL REMARKS

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

72. According to Article 64 (7) and (8) GDPR, the LV 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.

73. The LV 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)