Opinion 25/2021 on the draft decision of the competent supervisory authority of Lithuania regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)

Adopted on 20 July 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 requirements a supervisory authority establishes pursuant to Article 43(1)(a). 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 Lithuanian SA (hereinafter "LT SA") has submitted its draft accreditation requirements under Article 43 (1) (a) to the EDPB. The file was deemed complete on 28 May 2021.

2. The LT SA will perform accreditation of certification bodies to certify using GDPR certification criteria.

2 ASSESSMENT

2.1 General reasoning of the EDPB regarding the submitted draft decision

3. 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 LT SA is tasked by national law to carry out the accreditation of certification bodies. To this end, the LT SA has developed a set of requirements specifically for accreditation of certification bodies in conjunction with a set of certification criteria that is yet to be formally approved.

4. This assessment of LT SA's draft accreditation requirements is aimed at examining on variations (additions or deletions) from the Guidelines and notably their Annex 1. Indeed, according to the Guidelines, following the approach provided by the Annex (where practical) is a good practice, even where supervisory authorities perform accreditation pursuant to Article 43(1)(a), as it is the case here.

[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

Furthermore, the EDPB's Opinion is also focused on all aspects that may impact on a consistent approach regarding the accreditation of certification bodies.

5. 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.

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

8. This opinion does not reflect upon items submitted by the LT 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);

the Board is of the opinion that:

2.2.1 PREFIX

10. The Board acknowledges that the accreditation requirements drafted by the LT SA are presented as an Annex to the Description of the Procedure for Accreditation of Certification Bodies. The description of that procedure has not been provided to the EDPB since it is not a requirement for the accreditation of certification bodies *per se*.

2.2.2 GENERAL REMARKS

11. The Board notes that some terms in the LT SA's draft accreditation requirements are not used consistently with the Guidelines and the Annex, such as 'personal data protection operations' instead of 'personal data processing operations'; 'certification object' instead of 'object of certification'; 'the entity subject to certification' instead of 'the applicant' or 'the client'; 'earlier [versions]' instead of 'previous [versions]'; 'experience' instead of 'expertise'; 'conformity assessment' instead of 'evaluation'; "enable [the LT SA] to familiarize with" instead of "made fully accessible [to the SA]"; 'management body' instead of 'management system' etc. Moreover, in Section 7.1, paragraph 1, of draft accreditation requirements, the reference to Article 43(1)(b) of the GDPR and the 'additional requirements' established by the LT SA is not entirely accurate, since it is the LT SA which is competent to perform accreditation of certifications bodies pursuant to Article 43(1)(a) of the GDPR. In order to avoid confusion, the terms used should be aligned with the Guidelines and the Annex definitions, where possible, and used consistently. Therefore, with the aim to facilitate the assessment, the Board encourages the LT SA to amend the draft requirements accordingly.

2.2.3 GENERAL REQUIREMENTS FOR ACCREDITATION

12. The Board notes that, according to the general draft accreditation requirements in section 4.1.1 ("Legal responsibility"), the certification body must be able at any time to prove to the Inspectorate that "no bankruptcy proceedings have been instituted against the certification body, for example, by providing an extract from the Register of Legal Entities". However, the same clause is reproduced under the general requirements outlined in section 4.3 ("Liability and financing") with an additional reference to insolvency or liquidation proceedings along with bankruptcy. In this regard, the Board acknowledges that the aim in both cases is to make sure that the certification body is able to exercise the certification activity with full legal responsibility, including for example to pay compensations if necessary. Nevertheless, the Board encourages the LT SA to revise both requirements so as to avoid any redundancy and inconsistency.

13. With regard to section 4.1.2 ("Certification agreement") of the LT SA's draft accreditation requirements, the Board notes that the first paragraph states that the certification agreement shall be "in writing". In order to ensure that electronic certification agreements are also covered, the EDPB encourages the LT SA to replace "in writing" by "in written form" or equivalent wording.

14. In paragraph 1 of the said section, it is established that the certification agreement shall require that the applicant always complies with both the general certification requirements of the Standard ISO 17065 and the certification criteria established by the certification body and approved by the LT SA in accordance with Article 43(2)(b) and Article 42(5) of the GDPR. In this regard, since certification criteria may be established by scheme owners who do not necessarily act as a certification bodies, the EDPB encourages the LT SA to amend the draft accreditation requirements by replacing the term 'certification body' with 'scheme owner'. In addition, since according to with Article 43(2)(b) and Article 42(5) of the GDPR , the certification bodies may be accredited to conduct certification under the criteria approved by the competent SA, or even by the Board, if those criteria are identified as suitable for common certification and result in a European Data Protection Seal, the EDPB recommends amending the requirement so as to take into account that the applicant could be required to comply with those criteria approved by the Board at Union level.

15. Also in section 4.1.2, paragraph 2, it is stated that the certification agreement shall require that the applicant provides the SA with all necessary information "including confidential information on the certification procedure to the extent that it is related to compliance with personal data protection requirements". The Board considers that the wording of the draft requirement is not in line with the Annex - which refers to the transparency towards the SA "*with respect to the certification procedure including contractually confidential matters related to data protection compliance*" - and encourages the LT SA to redraft the requirement so as to reflect better what it is stated in the Annex.

16. Section 4.1.2, paragraph 3, of the LT SA's draft accreditation requirements, provides that the certification agreement shall not reduce the responsibility of the applicant "*or the certification body set forth in Regulation (EU) 2016/679***".** The Board believes that the reference to the compliance of the certification body with the GDPR is not a matter that should be included in the certification agreement and encourages the LT SA to delete it.

17. In paragraph 5 of section 4.1.2, it is expected that the certification agreement shall "*establish the applicable certification criteria and methods, criteria for assessment of the certification object (including assessment if the certification body has sufficient competence within the context of assessment of the certification object), deadlines, procedures and the responsibility of the entity subject to certification to follow the deadlines and procedures related to certification or renewal thereof provided for in the agreement, the procedure established by the certification body and, where applicable, other ISO standards*". The Board understands that for transparency reasons this requirement mentions in detail several aspects related to the certification procedure (criteria, methods, deadlines, procedures and responsibilities) going beyond those required in the Annex. However, for the sake of clarity, the Board encourages the LT SA to specify that the requirement can be met by including in the certification agreement a reference to the relevant documentation of the certification mechanism in which these aspects are described in detail.

18. Section 4.1.2 of the Annex, paragraph 8, provides that the certification agreement includes rules on the necessary precautions for the investigation of complaints. This element is not mentioned in the corresponding paragraph of section 4.1.2 of the LT SA's draft accreditation requirements among the

issues that certification agreement shall address. Hence, the Board recommends including such element in the draft accreditation requirements in line with the Annex.

19. Section 4.1.2 of the LT SA's draft accreditation requirements, paragraph 9, stipulates that the certification agreement shall refer to the applicant's obligation to notify the certification body of any breaches of the GDPR and other legal acts regulating personal data protection found by supervisory authorities or court which may affect conformity assessment. The second part of the paragraph states that "*The afore-mentioned information shall be provided immediately after information on the detected breach becomes available to the entity subject to certification*". The Board understands that the objective of the notification is to inform the certification body only of possible breaches that are established by a supervisory authority or a court which may affect the applicant's conformity assessment. However, if this is the case, the required information could not have been reported immediately by the applicant, after a breach was detected, as envisaged by the last sentence of paragraph 9. Therefore, the Board encourages the LT SA to delete the last sentence of the paragraph in order to avoid confusion.

20. Section 4.1.2 of the Annex, point 6, prescribes that the certification agreement, with respect to 4.1.2.2 lit. c No. 1 ISO/IEC 17065/2012, shall set out the rules of validity, renewal, and withdrawal pursuant to Articles 42(7) and 43(4) of the GDPR including rules setting appropriate intervals for re-evaluation or review (regularity) in line with Article 42(7) of the GDPR. However, in section 4.1.2, paragraph 10, of the LT SA's draft accreditation requirements, it seems that the certification agreement only needs to contain a statement as to how the conformity assessment rules have to be established "*including the rules related to regular conformity reassessment or review intervals*" according to Article 42(7) of the GDPR. Hence, the Board recommends amending this clause of the draft accreditation requirements so as to align it with the Annex.

21. Regarding paragraph 11 of section 4.1.2, the Board recommends referring to the impact of the withdrawal or suspension of the certification body's accreditation, not only on the 'entity subject to certification', but also on the certified entity in line with the Annex. In the same paragraph, a reference is included to the consequences for the data subjects. However, the LT SA omitted a reference to [where applicable] "the consequences for the customer [that] should also be addressed", as stated in the Annex. The Board therefore recommends the LT SA to replace the term 'data subjects' with 'customer', in order to align this requirement with the Annex.

22. With regard to paragraph 12 of section 4.1.2, the EDPB recommends adding a reference to the applicant's obligation to notify the certification body of significant changes in the applicant's products, processes and services concerned by the certification as in section 4.1.2 of the Annex, paragraph 10. In addition, the Board encourages amending the corresponding explanatory note, so as to clarify that the examples provided therein cover such changes.

23. In relation to "Management of impartiality", the Board notes that in section 4.2, paragraph 3, the LT SAs draft accreditation requirements state that the certification body shall confirm that it is not related to the LT SA or its employees. According to the Annex the risk of impartiality for the certification body may arise from the possible connection with the customer it assesses. Therefore, the EDPB recommends the LT SA to replace the reference to the Data Protection Inspectorate or its employees with the reference to the customer.

24. In the said section, several examples of conflicts of interests or partiality of the certification body are provided. The Board welcomes the use of examples to further clarify the content of the requirements. However, some of these examples are drafted in general term, as if they were requirements, without

providing elements that may guide the assessment of specific cases falling in the situations described in the examples. In particular, the draft accreditation requirements mention the case where the "*major part of turnover of the certification body consists of income from provision of certification services*" (point 5), as well as where "*the activities of the certification body are financed by the entity subject to certification*" (point 6). Both situations described in the examples could probably concern most of the certification bodies, given that they are not adequately circumscribed.

25. First of all, with regard to the circumstances described in these examples, a situation likely to give rise to a conflict of interest could rather be when the certification body obtains a large part of its revenue from one or very few applicants/clients. More in general, these examples should be redrafted in more specific terms or included in the text of the requirements themselves along with the necessary elements to lead the assessment of specific cases by defining better their scope of application. Hence, the Board recommends the LT SA to amend the said examples accordingly, taking into account that a situation likely to give rise to a conflict of interest could be when the certification body obtains a large part of its revenue from one or very few applicants/clients.

26. Section 4.3 of the LT SA'S draft accreditation requirements on "Liability and financing "envisages that the certification body shall provide the documents supporting that it has appropriate measures to cover the obligations related to its activities and that it is financially stable. Among the examples provided in this clause, the fact that the certification body "*has no debts related to payments to the State budget, for example, a certificate issued by the State Tax Inspectorate under the Ministry of Finance of the Republic of Lithuania*" is mentioned in paragraph 3. In this regard, the Board encourages the LT SA to clarify why these financial obligations, which are unrelated to the GDPR, are included in the draft accreditation requirements. More specifically, the scope of this example should be better defined by specifying that it refers to the case in which such financial obligations are likely to affect the financial stability of the certification body or in any case its ability to provide certification services.

27. Another example, provided in the same subsection, paragraph 4, refers to the case where "*accreditation bodies, competent supervisory authorities or courts of Lithuania or other Member States have not taken final decisions on the breaches related to the certification body's activities, management of accounts in respect of the certification body itself or its personnel*". Also in this regard, the Board encourages the LT SA to specify that the example refers to the case in which such decisions are likely to affect the financial stability of the certification body or in any case its ability to provide certification services.

28. Among the said examples, paragraph 5 refers to the situation where the certification body carries out an assessment of the risk arising from the provision of certification services and its impact on the entity subject to certification and approves the measures for elimination or mitigation of the identified risk. This clause does not seem to contain an additional requirement to item 4.3. of ISO 17065, but rather it seems to complement items 4.2.3, 4.2.4, 4.2.11 of the same standard. Therefore, for the sake of clarity, the Board encourages LT SA to amend the draft accreditation requirements accordingly.

29. With respect to the publicly available information in subsection 4.6 of the LT SA'S draft accreditation requirements, the EDPB recommends complementing the reference to the "information about complaint handling procedures following Article 43(2)(d) of the GDPR" with the information about "the appeals" in line with the Annex.

2.2.4 STRUCTURAL REQUIREMENTS

30. The Board observes that section 5.1 of the LT SA's draft accreditation requirements ("Organisational structure and top management") refers to the appointment of "a person responsible for compliance with personal data protection requirements and information management, application of security measures who has at least 2 years of work experience in the area of personal data protection" The functions of this person seem similar to those of a data protection officer. The Board encourages the LT SA to clearly set out the functions of this person.

31. Among the documents supporting conformity with the afore-mentioned requirements it is mentioned as an example: "*the scheme or description of the organisational structure specifying the duties, responsibilities, accountability of the persons participating in the conformity assessment. This document or a separate document shall also contain information specified in subclause 5.1.3 of the Standard ISO 17065."* The Board notes that this requirement closely reflects what is envisaged in item 5.1.2 of of ISO 17065 and encourages the LT SA to better clarify that this is only an example based on ISO 17065.

32. Another example included among such documents is the" scheme *or other description establishing the persons to which information is provided and what information is provided, for example, information on possible breaches, risks of conflicts of interests, received complaints etc. This paragraph shall apply when information is provided to several persons*". According to the Board, this example is vague and abstract and risks being ambiguous. Hence, the Board encourages the LT SA to delete the example.

2.2.5 RESOURCE REQUIREMENTS

33. With regard to the requirements of certification body personnel, in subsection 6.1, the EDPB observes that the "*knowledge related to personal data protection legislation*" or the "*experience in the area of personal data protection*", as well as the "*expert knowledge on the certification object*", or the "*knowledge about personal data technical and organisational security data protection measures*" should be 'relevant', 'ongoing' and 'appropriate' as required in the Annex. Moreover, the "*experience in identifying and implementing data protection measure"* for the *"employees responsible for certification decisions*" should be 'significant' as in the Annex. Therefore, the Board recommends the LT SA to amend their draft requirements accordingly.

34. As for personnel with technical expertise (paragraph 4), the draft accreditation requirements prescribe that the certification body "*has to demonstrate that they improve their qualification in the respective area related to technical and audit knowledge, participation in continuous professional development programs*". In this regard, the Board encourages the LT SA to replace the term 'improve' with 'maintain' so as to align this requirement with the Annex.

35. Concerning the personnel with legal expertise, the Board encourages the LT SA to clarify that the required years of professional experience have to be relevant for the tasks they will perform.

2.2.6 PROCESS REQUIREMENTS

36. The Board notes that paragraph 3 of section 7.1 ("General") of the LT SA's draft accreditation requirements includes the obligation of the certification body to notify to the LT SA of the decisions on certificates sought, prior to issuing, renewing or withdrawing certifications and to provide the SA with a copy of the summary of the conclusion on the assessment carried out. Moreover, section 7.6 ("Certification decision"), in paragraph 2, prescribes the certification body to verify, before taking a decision on issue (renewal) of a certificate, if the SA has not initiated any investigations against the applicant showing that it does not meet the certification criteria. In this regard, paragraph 5 of section 7.2 ("Application") already requires that information on whether an investigation is being carried out against the applicant is to be provided in the certification application.

37. The said requirements, read in conjunction with each other, seem to suggest that a supervision by the SA of certification decisions is entailed. However, on the basis of the explanations supplied by the LT SA, the Board understands that this does not mean that the SA would need to approve each and every decision of certification body. Thus, for the sake of clarity and legal certainty, the Board encourages the LT SA to clarify the aim of these requirements, specifying that they do not entail a supervision of each and every certification decision by the LT SA, but that the SA reserves the right to exercise the power to order the certification body not to issue certification, under Article 58 paragraph 2, lett. h) of the GDPR, if it is in possession of information concerning serious breaches of data protection rules and principles from which it derives that the applicant does not meet the certification criteria.

38. Paragraph 4 of section 7.2 ("Application") states that the application to obtain the certification shall specify "*if the certification object also covers transfer of personal data to third countries*" as well as "*personal data to be transferred, its recipients and personal data security measures which shall be applied in such case*". As part of the work program for 2020-2021, the Board is currently working on Guidelines on certifications as a tool for transfers. Since the Guidelines have not been adopted yet, the Board considers that the reference to the transfer of personal data to third countries in this requirement might create confusion and may need to be amended once the Guidelines are adopted. Therefore, the Board recommends deleting the said requirement as well as the reference to the transfer tools included in point 3 of the list of documents supporting conformity with the afore-mentioned requirement.

39. In section 7.3 ("Application review"), the Board recommends adding the obligation to have binding evaluation methods with respect to the ToE in the certification agreement as required in the Annex.

40. With respect to section 7.4 of the LT SA's draft accreditation requirements ("Evaluation"), the Board notes that a specific reference to the use of external experts for conformity assessment is included in paragraph 3, as stated in the Annex. In this regard, the Board encourages the LT SA to include a specific reference to the use of external experts who have been recognized by the certification body. In addition, 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 LT SA to amend the draft accreditation requirements accordingly.

41. As for paragraph 5 of the afore-mentioned section, the Board recommends amending the draft accreditation requirements to clarify that the obligation to set out in the certification mechanism how to inform the customer about nonconformities is placed on the certification body and not on the

applicant. More in general, the Board encourages the LT SA to redraft the requirement so as to align the wording with the Annex.

42. In section 7.5 ("Review") the draft accreditation requirement refers to the procedure for "*review and withdrawal of the conclusions drawn [by the certification body] in the course of the assessment in accordance with Articles 43(2) and 43(3) of Regulation (EU) 2016/679*" while the Annex mentions the procedures for "*regular review and revocation of the … certifications pursuant to Article 43(2) and 43(3)*" of the GDPR. Thus, the Board encourages the LT SA to replace the term 'conclusions' with 'certifications'.

43. According to paragraph 1 of section 7.8 of the draft accreditation requirements ("Directory of certified products"), the certification body shall publish information on, among others, the certified object (products, processes and services). In this regard, the Annex requires that the afore-mentioned information must be available internally and publicly available. Thus, the Board recommends the LT SA to amend the requirements in line with what it is stated in the Annex so as to clarify that, for instance, posting such information on a local intranet, would not comply with the requirements.

44. In paragraph 2 of section 7.10 ("Changes affecting certification"), among the changes affecting certification which must be assessed by the certification body, the LT SA's draft accreditation requirements mention the "*major changes in the personal data processing operations which are (were) certified*". For the sake of clarity, the Board encourages the LT SA to clarify the meaning of the said 'major changes' with regard to the client's processing operations.

45. In paragraph 5 of the same section the draft accreditation requirements refer to "*decisions, opinions, guidelines, recommendations or good practices adopted by the Board"*. To cover other types of documents that may be issued by the EDPB, the Board encourages the LT SA to add "and other documents" at the end of this clause.

46. As for section 7.12 ("Records") of the LT SA's draft accreditation requirements, the Board recommends including a reference to the obligation of the certification body to keep all documentation complete, comprehensible, up-to-date and fit to audit so as to align the draft accreditation requirements with the Annex.

2.2.7 MANAGEMENT SYSTEM REQUIREMENTS

47. Paragraph 2 of chapter VIII ("Management system requirements") of the LT SA's draft accreditation requirements states that "the management body shall cover the requirements set forth in paragraphs 9.3.3 and 9.3.4 hereof". The Board understands that the term the 'management body' be intended as the 'management system'. However, the reference to the requirements set forth only in paragraphs 9.3.3 and 9.3.4 risks to create ambiguity. Thus, for the sake of clarity and legal certainty, the Board recommends replacing the reference to the said paragraphs with a more general reference to the implementation of all draft requirements from the previous chapters.

48. With regard to paragraph 3 of the said chapter, the Board notes that the obligation of the certification body to disclose to the LT SA the management principles and their documented implementation during the accreditation procedure is not foreseen. The Board recommends the LT SA to amend the draft requirements, by including such obligation, as stated in the Annex.

2.2.8 FURTHER ADDITIONAL REQUIREMENTS

49. With regard to section 9.3.1 ("Communication between the certification body and its clients"), the Board underlines that the procedures and communication structures in place between the certification body and its customer should include the "maintenance" of the documentation of tasks and responsibilities by the accredited certification body. Therefore, the Board recommends the LT SA to add this element in the draft accreditation requirements as provided in the Annex.

50. The last sentence of section 9.3.3 ("Administration of examination of complaints") of the LT SA's draft accreditation requirements partially reflects the obligation under the Annex. Indeed, the Board considers that the SA not only have to be informed of relevant complaints and objections, but they have to be shared with the SA. Therefore, the Board recommends the LT SA to redraft the requirement by stating that relevant complaints and objections shall be shared with the LT SA the as Annex requires. Moreover, the Board encourages the LT SAs to replace the reference to "justified complaints" by "substantiated complaints", in order to provide more clarity.

3 CONCLUSIONS / RECOMMENDATIONS

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

52. Regarding 'general requirements for accreditation', the Board recommends that the LT SA:

1) amends the draft accreditation requirement in paragraph 1 of section 4.1.2 ("Certification agreement") so as to take into account that the applicant could be required to comply with the criteria of a common certification resulting in a European Data Protection Seal approved by the Board at Union level;

2) in paragraph 8 of in section 4.1.2, includes a reference to the rules on the necessary precautions for the investigation of complaints among the issues that the certification agreement shall address;

3) amends the draft accreditation requirements in paragraph 10 of section 4.1.2, so as to align it with the Annex;

4) regarding paragraph 11 of section 4.1.2, refers to the impact of the withdrawal or suspension of the certification body's accreditation on the certified entity and replaces the term 'data subjects' with 'customer', in order to align this requirement with the Annex;

5) with regard to paragraph 12 of section 4.1.2, adds a reference to the applicant's obligation to notify the certification body of significant changes in the applicant's products, processes and services concerned by the certification as in section 4.1.2 of the Annex, paragraph 10;

6) in section 4.2 ("Management of impartiality"), paragraph 3, replaces the reference to the Data Protection Inspectorate or its employees with the reference to the customer;

7) redrafts the examples concerning conflicts of interests or partiality of the certification body provided in points 5 and 6 of section 4.2, in more specific terms or includes them in

the text of the requirements, along with the necessary elements to lead the assessment of specific cases by defining better their scope of application, taking into account that a situation likely to give rise to a conflict of interest could be when the certification body obtains a large part of its revenue from one or very few applicants/clients;

8) with respect to the publicly available information in subsection 4.6, complements the reference to the "*information about complaint handling procedures following Article 43(2)(d) of the GDPR*" with the information about 'the appeals' in line with the Annex;

53. Regarding 'resource requirements', the Board recommends that the LT SA:

1) amends the draft requirements of certification body personnel in subsection 6.1, in accordance with the Annex;

54. Regarding 'process requirements', the Board recommends that the LT SA:

1) deletes the draft accreditation requirement in paragraph 4 of section 7.2 ("Application"), as well as the reference to the transfers tools included in point 3 of the list of documents supporting conformity with the afore-mentioned requirement;

2) in section 7.3 ("Application review"), adds the obligation to have binding evaluation methods with respect to the ToE in the certification agreement as required in the Annex;

3) with respect to section 7.4 ("Evaluation"), paragraph 3, explicitly states that the certification body will retain the responsibility for the decision-making, even when it uses external experts;

4) as for paragraph 5 of the afore-mentioned section, clarifies that the obligation to set out in the certification mechanism how to inform the customer about nonconformities is placed on the certification body and not on the applicant;

5) as for paragraph 1 of section 7.8 ("Directory of certified products"), amends the draft accreditation requirements in line with what is stated in the Annex so as to clarify that, for instance, posting such information on a local intranet, would not comply with the requirements;

6) as for section 7.12 ("Records"), includes a reference to the obligation of the certification body to keep all documentation complete, comprehensible, up-to-date and fit to audit so as to align the draft accreditation requirements with the Annex;

55. Regarding 'management system requirements', the Board recommends that the LT SA:

1) in paragraph 2 of Chapter VIII ("Management system requirements"), replaces the reference to paragraphs 9.3.3 and 9.3.4 with a more general reference to the implementation of all draft requirements from the previous chapters;

2) with regard to paragraph 3 of the said Chapter, amends the draft accreditation requirements, by including the obligation of the certification body to disclose to the LT SA the management principles and their documented implementation during the accreditation procedure, as stated in the Annex.

56. Regarding 'further additional requirements', the Board recommends that the LT SA:

1) with regard to section 9.3.1 ("Communication between the certification body and its clients"), adds a reference to the "maintenance" of the documentation of tasks and responsibilities by the accredited certification body as provided in the Annex;

2) redrafts the last sentence of section 9.3.3 ("Administration of examination of complaints") by stating that relevant complaints and objections shall be shared with the LT SA the as Annex requires.

4 FINAL REMARKS

57. This Opinion is addressed to the LT Supervisory Authority and will be made public pursuant to Article 64 (5)(b) GDPR.

58. According to Article 64 (7) and (8) GDPR, the LT 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.

59. The LT 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)