Opinion 13/2022 on the draft decision of the competent supervisory authority of Bulgaria regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)

Adopted on 4 July 2022

Table of contents

The European Data Protection Board

Having regard to Article 63, Article 64 (1c), (3) - (8) and Article 43 (3) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereafter "GDPR"),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018,[1]

Having regard to Article 10 and 22 of its Rules of Procedure of 25 May 2018,

Whereas:

(1) The main role of the Board is to ensure the consistent application of the Regulation 2016/679 (hereafter GDPR) throughout the European Economic Area. In compliance with Article 64.1 GDPR, the Board shall issue an opinion where a supervisory authority (SA) intends to approve the requirements for the accreditation of certification bodies pursuant to Article 43. The aim of this opinion is therefore to create a harmonised approach with regard to the requirements that a data protection supervisory authority or the National Accreditation Body will apply for the accreditation of a certification body. Even though the GDPR does not impose a single set of requirements for accreditation, it does promote consistency. The Board seeks to achieve this objective in its opinions firstly by encouraging SAs to draft their requirements for accreditation following the structure set out in the Annex to the EDPB Guidelines on accreditation of certification bodies, and, secondly by analysing them using a template provided by EDPB allowing the benchmarking of the requirements (guided by ISO 17065 and the EDPB guidelines on accreditation of certification bodies).

(2) With reference to Article 43 GDPR, the competent supervisory authorities shall adopt accreditation requirements. They shall, however, apply the consistency mechanism in order to allow generation of trust in the certification mechanism, in particular by setting a high level of requirements.

(3) While requirements for accreditation are subject to the consistency mechanism, this does not mean that the requirements should be identical. The competent supervisory authorities have a margin of discretion with regard to the national or regional context and should take into account their local legislation. The aim of the EDPB opinion is not to reach a single EU set of requirements but rather to avoid significant inconsistencies that may affect, for instance trust in the independence or expertise of accredited certification bodies.

(4) The "Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)" (hereinafter the "Guidelines"), and "Guidelines 1/2018 on certification and identifying certification criteria in accordance with article 42 and 43 of the Regulation 2016/679" will serve as a guiding thread in the context of the consistency mechanism.

(5) If a Member State stipulates that the certification bodies are to be accredited by the supervisory authority, the supervisory authority should establish accreditation requirements including, but not limited to, the requirements detailed in Article 43(2). In comparison to the obligations relating to the

[1] References to the "Union" made throughout this opinion should be understood as references to "EEA".

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 Bulgarian Supervisory Authority (hereinafter "BG SA") has submitted its draft accreditation requirements under Article 43 (1)(b) to the EDPB. The file was deemed complete on 28 March 2022. The BG SA will perform accreditation of certification bodies to certify using GDPR certification criteria.

2. In compliance with article 10 (2) of the Board Rules of Procedure, due to the complexity of the matter at hand, the Chair decided to extend the initial adoption period of eight weeks by a further six weeks.

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 BG SA is tasked by national law to carry out the accreditation of certification bodies. To this end, the BG 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 BG 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.

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 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.

7. 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.

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

9. This opinion does not reflect upon items submitted by the BG 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.

10. Taking into account that:

a. Article 43 (2) GDPR provides a list of accreditation areas that a certification body needs 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 GENERAL REMARKS

11. The Board considers that in particular, it should be clear that GDPR certification is only applicable to processing operations and controllers and processors. In addition, the Board considers that the draft accreditation requirements should clearly state that the GDPR has precedence over ISO/IEC 17065/2012, as stated in the Annex. The EDPB thus encourages the BG SA to amend the requirements accordingly.

12. The Board notes that section "terms and definitions" states that definitions are based and in compliance with the GDPR and the relevant EDPB Guidelines. However, some of the definitions 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"). Therefore, the Board encourages the BG SA to ensure that the terms defined in the GDPR and/or the Guidelines are reflected consistently in the accreditation requirements. 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 BG SA to clarify these terms and to ensure that clear and consistent wording is used thorough the document.

13. 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 BG SA to make the necessary changes in this regard (e.g. in subsection 7.1.1).

14. In general, the Board encourages the BG SA to ensure consistency of the wording throughout the text (e.g. "Commission for Personal Data Protection", "CPDP" or "Competent Supervisory Authority").

2.2.2 GENERAL REQUIREMENTS FOR ACCREDITATION

15. Concerning subsection 4.1.1 of the BG 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 that the BG SA amends the draft requirements accordingly.

16. Regarding point 9 of subsection 4.1.2 of the BG SA's accreditation requirements, the Board notes the inclusion of a reference to the consequences for the data subjects. However, the BG SA omitted a reference to [where applicable] "the consequences for the customer should also be addressed", as stated in the Annex. The Board therefore recommends that the BG SA replaces the term with "customer" or "client", in order to align the wording with the Annex.

17. The Board is of the opinion that point 12 of subsection 4.1.2 of the BG 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 BG SA and/or judicial authorities. Thus, the Board recommends that the BG SA makes such clarification.

18. 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 BG SA to clarify that, in addition to having rules preventing conflicts, there should be clear rules to manage identified conflicts of interests.

19. With respect to subsection 4.2.3 of the BG SA's draft accreditation requirements ("Management of impartiality"), the Board encourages the BG 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.

20. With regard to subsection 4.3 ("Liability and financing") of the BG SA's draft accreditation requirements, the Board notes that, in accordance with the Annex, the certification body shall demonstrate on a regular basis that it has the appropriate measures to cover its liabilities. The BG SA's draft accreditation requirements do not include the notion of "regular basis". However, since the requirement says that the measures shall cover all the validity period, the Board for sake of clarity encourages the BG SA to include directly such reference, in line with the Annex.

21. Regarding subsection 4.6.1 ("Publicly available information"), the Board recommends the BG SA to add missing element of the Annex that all certification procedures are also published and easily publicly available.

22. In addition, subsection 4.6.2 indicates that "information related to complaints on the compliance with the certification requirements, as well as, information regarding complaints on certificates' breaches, is publicly available". Which may suggest that BG SA requires the certification body to ensure that information about each individual complaint is publicly available, that is in contradiction with the Annex, which requires that at minimum information about complaints handling procedures

and appeals is made public pursuant to Article 43(2)(d). Therefore, the Board encourages the BG SA to reformulate this requirement accordingly in order to ensure that personal data included in single complaints will not be publicly available.

2.2.3 RESOURCE REQUIREMENTS

23. As a general remark, 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 BG SA to redraft this subsection taking into account the different substantive knowledge and/or experience requirements for evaluators and decision-makers, rather than the years of experience.

24. Regarding the educational requirements for personnel with technical expertise, the reference to a recognised protected title in the relevant regulated profession should be included. Thus, the EDPB recommends that the BG SA redrafts the requirements to clarify the above-mentioned element, in line with the Annex.

25. As regards the requirements for personnel responsible for evaluations, The Board recommends that the BG SA refers to professional experience in technical data protection as well.

26. Finally, regarding the education requirements for the technical personnel, the Board considers that the list of subjects is already tailored to the technical expertise required by the Annex. Therefore, the Board encourages the BG SA to delete the reference to “humanitarian, natural science” from the list of subjects regarding the university education of the technical personnel. In addition the Board encourages the BG SA to replace “and” by “or” before other areas.

27. According to the Annex personnel with legal expertise responsible for evaluation shall be registered as required by the Member State. Based on the explanations provided by the BG SA, the Board understands that such an obligation exists in Bulgaria. Therefore the Board recommends that the BG SA includes this requirement.

28. The Board takes note that for personnel with legal expertise “the Certification body shall use the proper procedures to ensure that the personnel specific expertise is updated taking into account the changes in the legal situation, the data protection risks and the current state of the technique and technology”. In order to avoid misunderstandings, the Board encourages the BG SA to delete word “proper”.

29. As regards section 6 point6 on representatives in the governing bodies and the individuals, who make the final decision in issuing the certificate, the Board recommends that the BG SA brings this requirement in line with the Annex by specifying “ shall have significant experiences in identifying and implementing data protection measures” instead of shall have significant professional experience in the personal data protection area.

30. In order to avoid misunderstandings, the Board encourage the BG SA to clarify the last paragraph of the section 6 of the draft accreditation requirements stating that “The above listed general requirements for the Certification body resources will be further specified in the Ordinance for the conditions and the procedure for accreditation and withdrawal of accreditation of Certification bodies, which will be adopted on the basis of these criteria”.

2.2.4 PROCESS REQUIREMENTS

31. In section 7 on process requirements, the Board recommends that the BG adds a reference to "*Notify the relevant CSAs before a certification body starts operating an approved European Data Protection Seal in a new Member State from a satellite office."* so as to bring this requirement in line with the Annex.

32. The Board encourages the BG SA to redraft subsection 7.2.1. of the accreditation requirements in order to ensure consistency by using term ToE instead of "Object of certification".

33. As regards subsection 7.2 of the BG SA's accreditation requirements, the Board underlines that the applicant shall always contain a description of the data transferred to other systems or organisations, regardless of their location. Therefore, the Board encourages the BG SA to amend the wording in order to avoid confusion.

34. Regarding subsection 7.2. 2 ("Application") of the BG SA's draft accreditation requirements, the Board notes that it includes the obligation to provide "Information regarding all ongoing or closed investigations before the CPDP against the Applicant". 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 BG SA to clarify that the investigation or regulatory action should be related to the scope of certification and the target of evaluation.

35. The Board encourages the BG SA to bring subsection 7.3.1 in line with the Annex, by adding " binding assessment methods".

36. The Board notes that the obligation to have procedures for the granting, regular review and revocation of the respective certifications pursuant to Article 43(2) and 43(3) (section 7.5 of the Annex) is not included in the BG SA's draft requirements. Thus, the Board recommends that the BG SA includes it in the requirement.

37. The Board recommends that the BG SA brings subsection 7.6 in line with subsection 7.6 of the Annex, by adding missing elements.

38. The Board notes that the second paragraph of subsection 7.6 of the BG SA's draft accreditation requirements includes the obligation to submit to the BG SA the draft decision with a summary, which should include description of the compliance with the current requirements and the certification grounds, and a declaration which states that the Applicant does not have any ongoing proceeding before CPDP, prior to issuing, renewing or validity extension of the certification. Based on the explanations provided by the BG 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 BG SA to include a clarification in that sense.

39. With regard to subsection 7.7 ("Certification documentation"), the Board notes that the BG SA's accreditation requirements do not include the last paragraph of section 7.7 of the Annex. The Board considers that these requirements should be in the text of the accreditation requirements and recommends that the BG SA amends the requirements in order to include the information.

40. In subsection 7.8 point 1 the Board recommends that the BG SA adds a meaningful description on the object of certification pursuant to the Guidelines.

41. The Board encourages the BG SA to add in section 7.8 point 2 the phrase "including version or functional status".

42. In addition the Board recommends that the BG SA clarifies in line with section 7.8 of the Annex that elements listed in subsection 7.8 (points 1-4) are part of the executive summary and must be publicly available.

43. With regard to the last sentence of subsection 7.8 of the BG SA's draft accreditation requirements, the Board notes that this section concerns the obligation to inform the CPDP upon request of the reasons for issuance or non-issuance of a certificate, whereas the requirement in subsection 7.8 of the Annex to the Guidelines contains an obligation to proactively inform the SA of the reasons for granting or revoking the certification. Therefore, the Board recommends that the BG SA amends the draft accordingly.

44. With regard to subsection 7.9 of the BG SA's draft accreditation requirements ("Surveillance"), the Board considers that the risks associated with the processing should be taken into account in order to determine how frequent monitoring is necessary. Therefore, the Board encourages the BG SA to include a risk-based approach with regard to the arrangements for surveillance.

45. With regard to subsection 7.10 of the BG 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 BG SA to include this possibility among the list of changes that might affect certification.

46. In addition, the Board notes that subsection 7.10 includes "data security breaches or data protection legislation infringements". The Board considers that, in order to avoid self-incrimination, the reference should be to infringements established by the BG SA or the competent judicial authority. Therefore, the Board encourages the BG SA to add the abovementioned reference. At the same time, in order to ensure clarity, the Board encourages the BG SA to specify that the data security breaches or data protection legislation infringements shall be taken into account only inasmuch as they relate to the certification.

47. Additionally, the Board observes that there is no reference to the change procedures to be agreed, as per subsection 7.10 of the Annex. The Board encourages the BG SA to include such reference and mention some of the procedures that could be put in place (e.g. transition periods, approvals process with the competent SA...).

48. Regarding the obligation to inform the BG SA of the reasons for the termination, reduction, suspension or withdrawal of a certification (subsection 7.11 of the BG SA's accreditation requirements), the Board encourages the BG SA to clarify that the information should be provided in writing.

49. In subsection 7.12, the Board recommends that the BG SA specify that the certification body should be required to keep all documentation complete, comprehensible, up-to-date and fit to audit in line with subsection 7.12 of the Annex.

50. In subsection 7.13 ("Complaints and appeals, Art. 43 (2) (d)"), the Board recommends that the BG SA adds the missing elements of subsection 7.13 of the Annex such as "how and to whom such confirmation must be given" and "which processes are to be initiated afterwards".

2.2.5 MANAGEMENT SYSTEM REQUIREMENTS

51. The Board understands that section 8 of the BG SA's draft accreditation requirements includes the obligation to disclose to the BG SA the management principles and their documented implementation during the accreditation procedure and, afterwards, at the request of the BG SA at any time during an investigation, as stated in the Annex. However wording of this section is not fully in line with paragraph

4 and 5, section 8 of the Annex. Therefore, the Board recommends that the BG SA brings this section fully in line with the Annex.

2.2.6 FURTHER ADDITIONAL REQUIREMENTS

52. The first sentence of subsection 9.1 ("Updating of evaluation methods") of the BG SA's draft accreditation requirements refers to "the context of evaluation under point 7.4 of ISO/IEC 17065/2012", which does not reflect the wording of subsection 9.1 of the Annex. Therefore, the Board recommends that the BG SA adds the reference to the evaluation under subsection 7.4 of the BG SA's accreditation requirements.

53. The Board considers that subsection 9.3.4 of the BG SA's draft accreditation requirements is not in line with subsection 9.3.4 of the Annex, in particular the reference to notification to customers in the event of suspension or withdrawal of the accreditation is missing. The Board recommends that the BG SA includes the missing elements, in line with the Annex.

3 CONCLUSIONS / RECOMMENDATIONS

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

55. Regarding 'general requirements for accreditation', the Board recommends that the BG SA:

    1) amends subsection 4.1.1 of the BG SA's draft accreditation requirements in order to ensure 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 as well as 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.
    2) replaces in point 9 of subsection 4.1.2 of the BG SA's accreditation requirements the term "data subject" with the term "customer", in order to align the wording with the Annex.
    3) makes clarification in point 12 of subsection 4.1.2 of the BG SA's draft accreditation requirements that the obligation of the applicant to inform the certification body of infringements of the GDPR should refer to infringements established by the BG SA and/or judicial authorities.
    4) adds in subsection 4.6.1 missing element of the Annex that all certification procedures are also published and easily publicly available.
    5) adds in subsection 4.6.2 that information about complaints handling procedures and appeals is made public pursuant to Article 43(2)(d).

56. Regarding 'resource requirements', the Board recommends that the BG SA:

    1) adds a reference to a recognised protected title in the relevant regulated profession into the education requirements for personnel with technical expertise in line with the Annex.

2) refers in the requirements for personnel responsible for evaluations to professional experience in technical data protection as well.

3) includes to the requirements that personnel with legal expertise responsible for evaluation shall be registered as required by BG law.

4) specifies in section 6 point 6 that representatives in the governing bodies and the individuals, who make the final decision in issuing the certificate "shall have significant experiences in identifying and implementing data protection measures".

57. Regarding 'process requirements', the Board recommends that the BG SA:

1) adds in section 7 a reference to "Notify the relevant CSAs before a certification body starts operating an approved European Data Protection Seal in a new Member State from a satellite office."

2) includes the obligation to have procedures for the granting, regular review and revocation of the respective certifications pursuant to Article 43(2) and 43(3) (subsection 7.5 Annex).

3) brings subsection 7.6 in line with subsection 7.6 of the Annex, by adding missing elements.

4) adds in subsection 7.7 ("Certification documentation") the last paragraph of section 7.7 of the Annex.

5) adds in subsection 7.8. point 1) " a meaningful description" on the object of certification pursuant to the Guidelines.

6) clarifies in line with subsection 7.8 of the Annex that elements listed in subsection 7.8 (points 1-4) are part of the executive summary and must be publicly available.

7) amends the last sentence of subsection 7.8 of the BG SA's draft accreditation requirements, that certification body is obliged to proactively inform the SA of the reasons for granting or revoking the certification.

8) specifies in subsection 7.12 that the certification body should be required to keep all documentation complete, comprehensible, up-to-date and fit to audit in line with subsection 7.12 of the Annex.

9) adds in subsection 7.13 missing elements of section 7.13 of the Annex such as "how and to whom such confirmation must be given" and "which processes are to be initiated afterwards".

58. Regarding 'management system requirements', the Board recommends that the BG SA:

1) brings section 8 fully in line with paragraph 4 and 5, section 8 of the Annex.

59. Regarding 'further additional requirements', the Board recommends that the BG SA:

1) adds a reference to the evaluation under subsection 7.4 of the BG SA's accreditation requirements in line with the wording of subsection 9.1. of the Annex.
2) includes in the subsection 9.3.4 of the BG SA's draft accreditation requirement reference to notification to customers in the event of suspension or withdrawal of the accreditation.
Final Remarks

4 FINAL REMARKS

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

61. According to Article 64 (7) and (8) GDPR, the BG 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.

62. The BG 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)