Opinion 11/2022 on the draft decision of the competent supervisory authority of Poland regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)

Adopted on 4 July 2022

Table of contents

The European Data Protection Board

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

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

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

Whereas:

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

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

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

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

(5) If a Member State stipulates that the certification bodies are to be accredited by the supervisory authority, the supervisory authority should establish accreditation requirements including, but not

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

limited to, the requirements detailed in Article 43(2). In comparison to the obligations relating to the accreditation of certification bodies by national accreditation bodies, Article 43 provides fewer details about the requirements for accreditation when the supervisory authority conducts the accreditation itself. In the interests of contributing to a harmonised approach to accreditation, the accreditation requirements used by the supervisory authority should be guided by ISO/IEC 17065 and should be complemented by the additional requirements a supervisory authority establishes pursuant to Article 43(1)(b). The EDPB notes that Article 43(2)(a)-(e) reflect and specify requirements of ISO 17065 which will contribute to consistency.[2]

(6) The opinion of the EDPB shall be adopted pursuant to Article 64 (1)(c), (3) & (8) GDPR in conjunction with Article 10 (2) of the EDPB Rules of Procedure within eight weeks from the first working day after the Chair and the competent supervisory authority have decided that the file is complete. Upon decision of the Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

HAS ADOPTED THE OPINION:

1 SUMMARY OF THE FACTS

1. The Polish SA (hereinafter "PL 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 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 XX SA, once they are approved by the PL SA, following an opinion from the Board on the draft requirements, to accredit certification bodies. The PL 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 PL 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

[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

issuing accreditation. In this specific case, the Board notes that the PL SA is tasked by national law to carry out the accreditation of certification bodies. To this end, the PL 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 PL 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 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 PL SA's draft accreditation requirements, it should be read as the Board not having any comments and not asking the PL SA to take further action.

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

11. 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

12. The Board notes that some terms, for instance section 7.4 of the draft requirements refer to "targets of assessment" instead of "targets of evaluation" and to the term "assessment" instead of "certification". The Board considers that these terms are not in accordance with the Guidelines. Therefore, the Board encourages the PL SA to modify such terms so to bring them in line with the Guidelines.

13. The Board welcomes the reference "The wide range of ISO/IEC 17065/2012, covering products, processes and services, should not lead to lowering or substitution of GDPR requirements" in section 1 of the draft requirements. However the Board is of the Opinion that the precedence of the GDPR over the ISO/IEC 17065/2012 should be made explicitly in the requirements, pursuant to Annex 1

14. The Board notes that in section 1 of the PL SA's draft accreditation requirements, the PL SA makes a distinction between controller, processor and manufacturers or the entity marketing a service product. The Board's understanding is that both manufacturers and the entity marketing a service or product are either controllers or processors, thus the Board is not concerned by this distinction.

2.2.3 GENERAL REQUIREMENTS FOR ACCREDITATION

15. With respect to section 4.1.2 of the PL SA's draft accreditation requirements, the Board notes that in paragraph 5 of this section, the requirement of the Guidelines "the certification program and other regulations must be observed and adhered to" is missing. Therefore, the Board recommends the PL SA to complete this requirement accordingly.

16. Regarding section 4.1.2 of the PL SA's draft accreditation requirements, the Board notes there is a reference to certification body's obligation to "indicate" the consequences to the Customer in paragraph 9. With respect to this requirement, section 4.1.2 para. 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 PL 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 PL SA's accreditation requirements should make clear that simply stating the consequences without addressing the potential next steps won't be sufficient. Thus, the Board encourages the PL 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.

17. With regard to the section 4.3 of the draft requirements, the Board welcomes the inclusion the reference on liability and finances "In addition to the requirement set out in point 4.3.1 of ISO/IEC 17065/2012, the PCA shall ensure on a regular basis that the Certification Body has appropriate measures (e.g. insurance or reserves) to cover its liabilities." However the Board wish to highlight that the PL SA ommitted to include that the cover of liabilities refers to the geographical regions in which the NAB operates. Therefore, the Board recommends the PL SA to add this element to this requirement so to align it with the Guidelines.

18. Regarding section 4.6 of the PL SA's draft accreditation requirements, the certification body is required to provide "1) all versions (current and previous) of the approved criteria used within the meaning of Article 42(5) of the GDPR (certification criteria) are published and easily publicly available, as well as all certification procedures, generally stating a relevant period of validity and 2) information on complaint and appeal procedures are made public in accordance with Article 43(2)(d) of the GDPR." The Board encourages the PL SA to add in the requirements that this is information shall be provided **at minimum**, according to section 4.6 ISO/IEC 17065/2012.

2.2.4 RESOURCE REQUIREMENTS

19. 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 PL 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.

20. In section 6.1 of the PL SA's draft accreditation requirements, it is mentioned that "the certification body is responsible for making decisions even if it is assisted by sub-contractors". Right below it is mentioned that the "subcontractors should not be involved in decision-making processes". The Board recommends the PL SA to modify this requirement so to clarify that when the certification body uses subcontractors the certification body is the one responsible for the decision-making.

2.2.5 PROCESS REQUIREMENTS

21. With regard to section 7.1(2) of the draft requirements, the Board underlines that, even when an EU Data Protection Seal has been approved, the certification body still has to notify the relevant CSAs before operating it in a new Member State from a satellite office. This is especially relevant, considering that accreditation of a certification body granting European Data Protection Seals may have to be carried out in each of the Members States where the certification body is established. 3 However, it shall be noted that the CSAs should be notified even in those cases in which the operation of an EU Data Protection Seal in a new Member State does not require a new accreditation. Therefore, the Board recommends the PL SA to include the above-mentioned reference. For example, the draft requirements could state the following (see proposed amendments in italics): "If the certification body intends to act in other Member States, it shall notify and, when necessary, obtain the necessary approval from the relevant competent authorities, including for the operation of a European Data Protection Seal in accordance with Article 42(5) of the GDPR".

22. Similarly, in the same section, the Board encourages the PL SA to bring the draft accreditation requirements in line with the Guidelines, by adding "from a satellite office", that is currently missing from the draft.

23. Concerning paragraph 4 of section 7.1(4) and 7.2(4) of the draft requirements of the PL SA's, the Board notes that It should be clear that such investigation should be linked with the scope of certification and the target of evaluation. Therefore, the Board recommends that the PL SA amend its requirement accordingly, by specifying that the investigation should be linked to the scope of certification and the target of evaluation.

24. In section 7.4(1) the Board encourages the PL SA to add the missing term "concerned" before the data subjects so to bring this requirement in line with the Guidelines.

25. In section 7.4(2) the Board encourages the PL SA to replace the term "applicants" with "controller and processor".

26. In section 7.4(2) the Board notes that this reference "*However, the certificate itself will not be a sufficient proof and the Certification Body shall be obliged to verify compliance with the criteria in relation to the object of the assessment*" misses an element provided in the criteria (i.e. that this is not sufficient to completely replace partial evaluations). The Board recommends the PL SA to add this element to the draft requirements so to bring them in line with the Guidelines.

27. In the same section, the last part of the paragraph from the Guidelines is missing "...*a certification statement or similar certification certificates should not be considered sufficient to replace a report*'." The Board recommends the PL SA to complete the requirement accordingly.

28. In section 7.8 “directory of certified products” the Board recommends the PL SA to modify the draft requirements and clearly state that the certification body shall inform not only the Supervisory authority of the reasons for granting or revoking or refusing the requested certification, but also any other competent supervisory authorities.

29. The Board welcomes, in section 7.10 of the draft accreditation requirements, the inclusion of personal data breaches and infringements of the GDPR in the list of changes that can affect certification. However, in order to ensure clarity, the Board encourages the PL SA to specify that the data breaches or infringements of the GDPR shall be taken into account only inasmuch as they relate to the certification.

30. With regards to the section 7.11 of the draft accreditation requirements on “termination, reduction, suspension or withdrawal of certification”, regarding the obligation of the certification body to inform the supervisory authority of the measures taken about the continuation, restriction, suspension and revocation of certification, it is not specified that this should be in writing. The Board thus encourages the PL SA to clarify this requirement by adding that this information obligation will take place in writing.

2.2.6 MANAGEMENT SYSTEM REQUIREMENTS

31. With regard to section 8 of the draft accreditation requirements on “management systems requirements” of the draft accreditation requirements, the Board notes that the below two paragraphs of the Guidelines (section 8) are missing:

    1. These management principles and their documented implementation must be transparent and be disclosed by the accredited certification body pursuant in the accreditation procedure pursuant to Article 58 and thereafter at the request of the data protection supervisory authority at any time during an investigation in the form of data protection reviews pursuant to Art. 58(1)(b) or a review of the certifications issued in accordance with Article 42(7) pursuant to Article 58(1)(c).

    2. In particular, the accredited certification body must make public permanently and continuously which certifications were carried out on which basis (or certification mechanisms or schemes), how long the certifications are valid under which framework and conditions (recital 100).

    Thus the Board recommends the PL SA to add these two paragraphs so to complete the draft requirements.

2.2.7 FURTHER ADDITIONAL REQUIREMENTS

32. With respect to 9.3.1 of the draft accreditation requirements, the Board encourages to clarify that it is the responsibility of the certification body and add not only customers but also applicants.

3 CONCLUSIONS / RECOMMENDATIONS

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

34. Regarding ‘general remarks’, the Board recommends that the PL SA:

1) completes the requirement of section 4.1.2 (paragraph 5) by adding that the "certification program and other regulations must be observed and adhered to it".

2) adds to section 4.3 of the requirements that the cover of liabilities refers also to geographical regions that the NAB operates.

35. Regarding 'resource requirements', the Board recommends that the PL SA:

1) modifies the requirement of section 6.1 so to clarify that when the certification body uses sub-contractors the certification body is the one responsible for the decision-making.

36. Regarding 'process requirements', the Board recommends that the PL SA:

1) includes a reference in section 7.1(2) to the fact that even when an EU Data Protection Seal is approved, the certification body still has to notify the relevant CSAs before operating in a new Member state from a satellite office.

2) amends the requirement of section 7.1(3) and 7.2(4) by specifying that the investigation should be linked to scope of certification and target of evaluation.

3) includes in section 7.4(2), in addition to the reference "However, the certificate itself will not be a sufficient proof and the Certification Body shall be obliged to verify compliance with the criteria in relation to the object of the assessment", that this is not sufficient to completely replace partial evaluations.

4) completes the last paragraph of the same section, by adding that "...a certification statement or similar certification certificates should not be considered sufficient to replace a report'."

5) modifies the draft requirements in section 7.8 and clearly state that the certification body shall inform not only the Supervisory authority of the reasons for granting or revoking or refusing the requested certification, but also any other competent authorities.

37. Regarding 'management system requirements', the Board recommends that the PL SA:

1) adds, in section 8 of the draft requirement, the two paragraphs, that comparing to the Guidelines, section 8 are missing.

4 FINAL REMARKS

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

39. According to Article 64 (7) and (8) GDPR, the PL 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.

40. The PL 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)