Opinion 38/2023 on the draft decision of the competent supervisory authority of Slovenian regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)

Adopted on 21 December 2023

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 Slovenian (hereinafter "SI SA") has submitted its draft accreditation requirements under Article 43 (1)(b) to the EDPB. The file was deemed complete on 26 October 2023. The SI 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 SI SA, once they are approved by the SI SA, following an opinion from the Board on the draft requirements, to accredit certification bodies.

2 ASSESSMENT

2.1 General reasoning of the EDPB regarding the submitted draft decision

2. The purpose of this opinion is to assess the accreditation requirements developed by a SA, either in relation to ISO 17065 or a full set of requirements, for the purposes of allowing a national accreditation body or a SA, as per article 43(1) GDPR, to accredit a certification body responsible for issuing and renewing certification in accordance with article 42 GDPR. This is without prejudice to the tasks and powers of the competent SA. In this specific case, the Board notes that the SI SA has decided to resort to its national accreditation body (NAB) for the issuance of accreditation, having put together additional requirements in accordance with the Guidelines, which should be used by its NAB when issuing accreditation.

3. This assessment of SI SA's additional accreditation requirements is aimed at examining on variations (additions or deletions) from the Guidelines and notably their Annex 1. Furthermore, the EDPB's

[2] Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation, par. 39. Available at: https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_en

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

4. It should be noted that the aim of the Guidelines on accreditation of certification bodies is to assist the SAs while defining their accreditation requirements. The Guidelines' Annex does not constitute accreditation requirements as such. Therefore, the accreditation requirements for certification bodies need to be defined by the SA in a way that enables their practical and consistent application as required by the SA's context.

5. The Board acknowledges the fact that, given their expertise, freedom of manoeuvre should be given to NABs when defining certain specific provisions within the applicable accreditation requirements. However, the Board considers it necessary to stress that, where any additional requirements are established, they should be defined in a way that enables their practical, consistent application and review as required.

6. The Board notes that ISO standards, in particular ISO 17065, are subject to intellectual property rights, and therefore it will not make reference to the text of the related document in this Opinion. As a result, the Board decided to, where relevant, point towards specific sections of the ISO Standard, without, however, reproducing the text.

7. Finally, the Board has conducted its assessment in line with the structure foreseen in Annex 1 to the Guidelines (hereinafter "Annex"). Where this Opinion remains silent on a specific section of the SI SA's draft accreditation requirements, it should be read as the Board not having any comments and not asking the SI SA to take further action.

8. This opinion does not reflect upon items submitted by the SI SA, which are outside the scope of article 43 (2) GDPR, such as references to national legislation. The Board nevertheless notes that national legislation should be in line with the GDPR, where required.

2.2 Main points of focus for the assessment (art. 43.2 GDPR and Annex 1 to the EDPB Guidelines) that the accreditation requirements provide for the following to be assessed consistently:

a. addressing all the key areas as highlighted in the Guidelines Annex and considering any deviation from the Annex.

b. independence of the certification body

c. conflicts of interests of the certification body

d. expertise of the certification body

e. appropriate safeguards to ensure GDPR certification criteria is appropriately applied by the certification body

f. procedures for issuing, periodic review and withdrawal of GDPR certification; and

g. transparent handling of complaints about infringements of the certification.

9. Taking into account that:

   a. Article 43 (2) GDPR provides a list of accreditation areas that a certification body need to address in order to be accredited;

   b. Article 43 (3) GDPR provides that the requirements for accreditation of certification bodies shall be approved by the competent Supervisory Authority;

   c. Article 57 (1) (p) & (q) GDPR provides that a competent supervisory authority must draft and publish the accreditation requirements for certification bodies and may decide to conduct the accreditation of certification bodies itself;

   d. Article 64 (1) (c) GDPR provides that the Board shall issue an opinion where a supervisory authority intends to approve the accreditation requirements for a certification body pursuant to Article 43(3);

   e. If accreditation is carried out by the national accreditation body in accordance with ISO/IEC 17065/2012, the additional requirements established by the competent supervisory authority must also be applied;

   f. Annex 1 of the Guidelines on Accreditation of Certification foresees suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a certification body by the National Accreditation Body;

   the Board is of the opinion that:

2.2.1 PREFIX

10. The Board acknowledges the fact that terms of cooperation regulating the relationship between a National Accreditation Body and its data protection supervisory authority are not a requirement for the accreditation of certification bodies *per se*. However, for reasons of completeness and transparency, the Board considers that such terms of cooperation, where existing, shall be made public in a format considered appropriate by the SA.

2.2.2 GENERAL REMARKS

11. The Board notes that the SI SA in its draft accreditation requirements, section "terms and definitions" mentions that the latter are the terms and definitions provided in the GDPR and the EDPB Guidelines 1/2018. However, some of the definitions, such as the one on accreditation, do not correspond to the definitions provided in the EDPB Guidelines. Therefore, the Board encourages the SI SA to ensure that the terms defined in the Guidelines are reflected consistently in the accreditation requirements.

2.2.3 GENERAL REQUIREMENTS FOR ACCREDITATION

12. Concerning the requirement of legal responsibility (subsection 4.1.1), the Board takes note of the fact that the SI SA requires that the certification body "shall be able to demonstrate evidence of the GDPR and the Personal Data Protection Act". In order to ensure an adequate assessment and implementation of this requirement and strengthen it, the Board recommends the SI SA to replace "shall be able to provide evidence by "shall provide evidence".

13. With respect to section 4.2 of SI SA's draft accreditation requirements on "management of impartiality", the Board acknowledges the insertion by the SI SA of the requirement to prevent conflicts of interest. However, the Board encourages the SI SA to also include in is accreditation requirements rules to manage conflicts of interests, when such conflicts have been identified.

2.2.4 RESOURCE REQUIREMENTS

14. 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 SI 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.

15. Regarding section 6.1. of the SI SA's draft accreditation requirements, the Board notices that for the personnel with technical, the reference to the fact that the qualification shall be related to the relevant regulated profession, in accordance with the Guidelines, is missing. Therefore, the Board encourages the SI SA to modify this requirement accordingly, bringing them it line with the Guidelines.

16. Similarly, in the same section, the Board takes note of the Board notices that both for experience of the personnel with technical and legal expertise, the SI SA refers to "comprehensive" instead of, as in accordance with the Guidelines", "significant" experience. The Board encourages the SI SA modify these requirements so to bring them in line with the Guidelines.

17. The Board takes note of all the conditions that the personnel with legal expertise must meet. However, the SI SA misses to mention that the degree in law from a Slovenian or foreign university shall be "for at least eight semesters, including the academic degree Master (LLM)". The Board recommends the SI SA to add this in its accreditation requirements in line with the Guidelines.

2.2.5 PROCESS REQUIREMENTS

18. With reference to section 7.3 on application review, the SI SA makes reference to section 7.3.1 (e) of ISO 17065. However, in the Guidelines it is mentioned section 7.3 (3). The Board encourages the SI SA to modify these requirements so to bring them in line with the Guidelines.

19. Regarding the section 7.11 of the SI SA's draft accreditation requirements, the Board notes that the SI SA makes reference to non-compliance with the certification in case "significant data breaches" relating to the scope of the certification and the ToE. The Board understands by this requirement that in case that a significant data breach, related with the scope of the certification and the ToE, occurs, which indicates, by its nature, that the client had not taken appropriate measures as expected according to its certification, in the sense that , if the relevant certification requirements were indeed properly implemented, such a data breach would not have been occurred, then this should be considered as non-compliance with the certification, and appropriate actions should be taken by the certification body. The Board encourages the SI SA to clarify in its accreditation requirement.

2.2.6 MANAGEMENT SYSTEM REQUIREMENTS

20. In section 8 of the SI SA's draft accreditation requirements on "management system requirements" the element of the fact that the disclosure shall be made "by the accredited certification body pursuant to Article 58 GDPR" is missing. The Board encourages the SI SA to modify this requirement and bring it in line with the Guidelines accordingly.

3 CONCLUSIONS / RECOMMENDATIONS

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

22. Regarding 'general requirements for accreditation', the Board recommends that the SI SA:

    1) replaces under section 4.1.1. the reference to the fact that the certification body shall be able to demonstrate evidence of the GDPR and Personal Data Act with a reference to the fact the certification body shall provide evidence and not only be able to do so.

23. Regarding 'resource requirements', the Board recommends that the SI SA:

    1) adds to the requirement that the degree in law from a Slovenian or foreign university shall be "for at least eight semesters, including the academic degree master (LLM)", in order to bring this requirement in line with the Guidelines.

4 FINAL REMARKS

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

25. According to Article 64 (7) and (8) GDPR, the SI 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.

26. The SI 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

(Anu Talus)