Opinion 19/2021 on the draft decision of the competent supervisory authority of Hungary regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)

Adopted on 1 June 2021

Table of contents

The European Data Protection Board

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

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

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

Whereas:

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

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

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

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

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

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

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

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

HAS ADOPTED THE OPINION:

1 SUMMARY OF THE FACTS

1. The Hungarian Supervisory Authority (hereinafter "HU SA") has submitted its draft accreditation requirements under Article 43 (1)(b) to the EDPB. The file was deemed complete on 06 April 2021. The HU 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 HU SA, once they are approved by the HU 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 HU 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 HU 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 HU SA's draft accreditation requirements, it should be read as the Board not having any comments and not asking the HU SA to take further action.

8. This opinion does not reflect upon items submitted by the HU 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 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 HU SA to make the necessary changes in this regard (e.g. in section 7.4, 2nd, 5th and 6th paragraphs; section 7.6, 1st paragraph; section 7.7, 3rd paragraph; section 7.11, 1st paragraph; sections 7.12, 7.13 and 9.3.3)

12. In addition, the Board encourages the HU SA to use consistent wording and ensure that the requirements are drafted in a way that ensure clarity. In this regard, the Board notes that, for example, paragraph 3 of section 4.1.2 could refer to the powers of the NAIH “which is competent” in line with the GDPR, section 7.1.1 could refer to the additional requirements “of the NAIH”; section 4.2 should refer to “Regulation” 765/2008/EC. In addition, for the sake of clarity, the references to “the competent SA” should be replaced by “HU SA” or “the NAIH” in section 9.3.3.

2.2.3 GENERAL REQUIREMENTS FOR ACCREDITATION

13. With regard to section 4.1.1 of the HU SA's draft accreditation requirements, and in particular, the last sentence of the second paragraph, the Board considers that the reference to the subject matter of the ToE is not entirely correct in this case, since the requirement is related to the accreditation of the certification bodies and not to their certification activities. Therefore, the Board encourages the HU SA to delete the said reference in the last part of the requirement.

14. Regarding section 4.1.2, point 7, the EDPB notes that the HU SA's draft accreditation requirements establish that the certification agreement shall allow the certification body to "disclose all information necessary to the EDPB and NAIH for granting certification". Whereas the EDPB welcome the explicit reference to the HU SA, which provides clarity, the reference to the EDPB seems less accurate, given that article 42(8) GDPR does not specify the manner in which the EDPB will collate the information. Thus, the EDPB considers that the wording of the Annex, which provide for more flexibility, is more appropriate and encourages the HU SA to redraft the requirements in this line.

15. With regard to section 4.2 ("Management of impartiality"), the Board encourages the HU 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.

2.2.4 RESOURCE REQUIREMENTS

16. Concerning certification body personnel (section 6.1), the Board notes that the requirements follow the Annex. In this respect, the Board is of the Opinion that, with regard to the expertise of the certification body, the emphasis should be put on the different type of substantive expertise and experience. Specifically, the Board considers that the competence requirements for evaluators and decision-makers should be tailored taking into account the different tasks that they perform. In the Board's opinion, 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. On this respect, the Board considers that the requirements for personnel with technical expertise and for personnel with legal expertise should be more aligned, so as to avoid the situation in which personnel with technical expertise have significantly less expertise than personnel with legal expertise. Instead, the focus should be made on the differences between evaluators and decision-makers in terms of their expertise and experience. Considering this, the Board encourages the HU SA to redraft this section taking into account the different substantive knowledge and/or experience requirements for evaluators and decision-makers.

17. With regard to the legal personnel in charge of certification decisions, the Board notes that the HU SA's draft accreditation requirements determine a minimum of five years of professional experience in data protection law. In this regard, the Annex refers to "significant" professional experience, which encompasses not only quantitative elements but also qualitative ones. Thus, in order to ensure clarity, the Board encourages the HU SA to clarify that the required years of professional experience have to be relevant for the tasks they will perform.

2.2.5 PROCESS REQUIREMENTS

18. Section 7.1 par. 2 of the HU SA's draft accreditation requirements establishes the obligation to notify the HU SA before a certification body starts operating an approved European Data Protection Seal in a new Member State from a satellite office. The EDPB notes that this obligation is towards all the competent supervisory authorities and recommends the HU SA to amend the draft accordingly.

19. Furthermore, the Board notes that the use of external experts contracted by the certification body is foreseen in the HU SA's draft accreditation requirements. The Board considers that the draft accreditation requirements should explicitly state that the certification body will retain the responsibility for the decision-making, even when it uses external experts. Therefore, the Board recommends the HU SA to amend the draft accordingly.

20. The Board notes that the second paragraph of section 7.6 of the HU SA's draft accreditation requirements ("certification decision") includes the obligation to submit the draft approval to the HU SA, prior to issuing or renewing certification. Based on the explanations provided by the HU SA, the Board understand that the intention of this requirement is to increase transparency and, in case that the HU SA decides, on the basis of the information, to start an investigation, it will not suspend the certification process. The Board encourages the HU SA to include a clarification in that sense.

21. With regard to last paragraph of section 7.6 ("Certification decision"), the Board encourages to clarify that the investigations or procedure referred which may prevent certification being issued are those related to the target of evaluation or the scope of the certification.

22. Finally, with regard to section 7.9 ("Surveillance"), the EDPB notes that the draft requirements do not establish a specific period for the monitoring. In this regard, the Board considers that, when determining the periodicity of the surveillance, the risk associated with the processing should be taken into account. Even in those cases where a specific frequency for the monitoring is determined, a risk-based approach is necessary to assess whether a more frequent monitoring is needed. Thus, the EDPB encourages the HU SA to introduce a risk-based approach in order to determine the frequency of the surveillance. This does not prevent the HU SA to also include minimum deadlines for monitoring, combined with a risk-based approach.

3 CONCLUSIONS / RECOMMENDATIONS

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

24. Regarding 'process requirements', the Board recommends that the HU SA:

    1) amend section 7.1, par. 2 in order to refer to all the competent supervisory authorities.

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

4 FINAL REMARKS

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

26. According to Article 64 (7) and (8) GDPR, the HU 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.

27. The HU 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)