Opinion 14/2020 on the draft decision of the competent supervisory authority of Ireland regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)

Adopted on 25 May 2020

Adopted

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 1 to the EDPB Guidelines 4/2018 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) GDPR. In comparison to the obligations relating to the accreditation of certification bodies by national accreditation bodies, Article 43 GDPR 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) GDPR. The EDPB notes that Article 43(2)(a)-(e) GDPR 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 Irish Supervisory Authority (hereinafter "IE SA") has submitted its draft accreditation requirements under Article 43 (1)(b) to the EDPB. The file was deemed complete on 13 February 2020. The IE national accreditation body (INAB) will perform accreditation of certification bodies to certify using GDPR certification criteria. This means that the INAB will use ISO 17065 and the additional requirements set up by the IE SA, once they are approved by the IE SA, following an opinion from the Board on the draft requirements, to accredit certification bodies.

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 IE 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.

[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

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

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

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

2) independence of the certification body

3) conflicts of interests of the certification body

4) expertise of the certification body

5) appropriate safeguards to ensure GDPR certification criteria is appropriately applied by the certification body

6) procedures for issuing, periodic review and withdrawal of GDPR certification; and

7) 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 (Section 0 of the IE SA's draft accreditation requirements)

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 TERMS AND DEFINITIONS

12. The Board notes that the reference to the guidelines on accreditation as "WP 261" is not updated. The EDPB adopted the Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679). Therefore, the Board encourages the IE SA to amend the wording and refer to the Guidelines 4/2018.

2.2.3 GENERAL REMARKS

13. The Board notes that the IE SA's draft requirements refer repeatedly to the "competent supervisory authority". Since the competent SA in this case is the IE SA, the Board encourages the IE SA to replace the reference by "the DPC" or "the IE SA" in order to avoid confusion.

14. The Board acknowledges that the IE SA's draft requirements include a section on terms and definitions. However, some of the terms are not used consistently throughout the document (e.g.

"object of evaluation" and "ToE"). In order to avoid confusion, the Board encourages the IE SA to use consistent terminology in the draft requirements.

2.2.4 GENERAL REQUIREMENTS FOR ACCREDITATION (Section 4 of the draft accreditation requirements)

15. With regard to clause 7 of subsection 4.1.2 of the IE SA's draft accreditation requirements, the Board considers that the wording is slightly unclear with regard to whom the reasons for approving certification are provided. Moreover, the reference to "facilitating" the register is also unclear. Therefore, the Board encourages the IE SA to redraft it in a way that provides more clarity.

2.2.5 STRUCTURAL REQUIREMENTS (Section 5 of the draft accreditation requirements)

16. The Board observes that the IE SA's draft accreditation requirements make reference to the appointment of "a person with the relevant seniority with responsibility for overseeing data protection compliance and information governance." The reference to the relevant seniority should be clarified in terms of experience and the scope of authority. Moreover, the functions of this figure seem similar to those of a data protection officer. The Board encourages the IE SA to clearly set out the functions of this figure and to specify the relevant experience.

2.2.6 RESOURCE REQUIREMENTS (Section 6 of the draft accreditation requirements)

17. Concerning certification body personnel (subsection 6.1), the Board notes that the requirements for personnel with technical expertise responsible for making decisions include having at least 5 years of professional experience related to the subject matter of certification, whereas the personnel responsible for evaluations should have at least2 years of professional experience. Similarly, personnel with legal expertise taking decisions must have at least 5 years of professional experience, whereas those in charge of evaluations must have at least 2 years of experience. The Board notes that the required minimum years of professional experience between the personnel in charge of decision-making and the personnel in charge of evaluation differ significantly. In this regard, the Board considers that the emphasis should be put on the different type of expertise rather than on the number of years of professional experience. 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. Considering this, the Board encourages the IE SA to make more emphasis on the different substantive knowledge and/or experience for evaluators and decision-makers and to reduce the divergences in the years of experience required for them.

2.2.7 PROCESS REQUIREMENTS (Section 7 of the draft accreditation requirements)

18. With regard to subsection 7.10 of the IE SA's draft accreditation requirements ("Changes affecting certification"), the Board observes that there is no reference to the change procedures to be agreed, as per section 7.10 of the Annex. The Board encourages the IE 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...). Additionally, the Board considers that changes in the state of art are also relevant and might affect certification. Therefore, the Board encourages the IE SA to include this possibility among the list of changes affecting certification. Finally, the Board welcomes 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 IE 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.

19. Regarding the changes affecting certification (subsection 7.10 of the IE SA's draft requirements) and, in particular, the fifth bullet point, the Board notes that the IE SA refers to "applicable binding decisions of the European Data Protection Board" and also to Article 39 of the EDPB Rules of Procedure, which includes "all final documents adopted by the EDPB". In order to ensure a clear understanding of what is meant by "decisions of the European Data Protection Board", the Board encourages the IE SA to clarify the reference. An example could be to refer to "documents adopted by the European Data Protection Board".

20. The Board observes that subsection 7.11 of the IE SA's draft requirements (termination, restriction, suspension or withdrawal of certification) does not contain the obligation of the certification body to accept decisions and orders from the IE SA to withdraw or not to issue certification to an applicant if the requirements for certification are not or no longer met. Therefore, the Board recommends the IE SA to include such obligation.

3 CONCLUSIONS / RECOMMENDATIONS

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

22. Regarding 'process requirements' the board recommends that the IE SA:

    1) include, in subsection 7.11, the obligation of the certification body to accept decisions and orders from the IE SA to withdraw or not to issue certification to an applicant if the requirements for certification are not or no longer met.

4 FINAL REMARKS

23. This opinion is addressed to the IE SA and will be made public pursuant to Article 64 (5)(b) GDPR.

24. According to Article 64 (7) and (8) GDPR, the IE 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.

25. The IE 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)

Adopted