Opinion 4/2020 on the draft decision of the competent supervisory authority of the United Kingdom regarding the approval of the requirements for accreditation of a certification body pursuant to Article 43.3 (GDPR)

Adopted on 29 January 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 Article 51 (1b) of Directive 2016/680 EU on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (hereafter "Law Enforcement Directive").

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.

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

(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 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 UK SA has submitted its draft accreditation requirements under Article 43 (1)(b) to the EDPB. Following a decision deeming the file complete, it was broadcasted on 25 October 2019. The UK national accreditation body (NAB), UKAS, 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 SA, once they are approved by the 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

[2] Para. 39 Guidelines: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_en.pdf

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 UK 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.

4. This assessment of UK SA's additional accreditation requirements is aimed at examining on variations (additions or deletions) from the Guidelines and notably the Annex. 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. Where this Opinion remains silent on a specific section of the UK SA's draft accreditation requirements, it should be read as the Board not having any comments and is not asking the UK SA to take further action.

9. This opinion does not reflect upon items submitted by the UK 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 (Section 0 of the draft additional 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.

12. The Board takes note of the fact that the UK SA is putting in place such terms of cooperation with its NAB and that said terms will be made available on the website of the UK SA once finalised.

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

13. Concerning the requirement of legal responsibility (subsection 4.1.1), the Board takes note of the fact that the UK SA requires that the Certification Body (CB) being accredited "*should be able to provide evidence of compliance as required during the accreditation process*" with the GDPR and the UK Data Protection Act 2018. In order to ensure an adequate assessment and implementation of this

requirement, the Board encourages the UK SA to replace "*should be able to provide evidence*" by "shall provide evidence". Therefore, the Board recommends that the UK SA amends the draft accordingly.

14. Concerning the certification agreement (subsection 4.1.2) and, in particular, requirement number 8, (number 9 in the Annex) the Board takes note of the fact that the UK SA created a reworded version of part of the requirement foreseen in Annex 1 of the Guidelines. The UK SA, however, omitted a reference to [where applicable] "the consequences for the customer should also be addressed". The Board therefore recommends the UK SA to add the missing part of the requirement mentioned above.

15. Concerning the use of data protection seals and marks (subsection 4.1.3), the Board notes that the UK SA requests that a copy "*of the seal/mark/logo should be provided to the ICO for their records*." Given that seals, marks and logos are handled not only by the certification body, but also by the scheme owner, the Board encourages the UK SA to refer also to any seals, marks and logos foreseen in any UK SA-approved certification schemes.

2.2.3 RESOURCE REQUIREMENTS (Section 6 of the draft additional accreditation requirements)

16. Concerning certification body personnel (subsection 6.1) and, in particular, point 6, the Board takes note of the fact that the UK SA has foreseen that "*Personnel responsible for certification decisions must have significant professional experience in identifying and implementing data protection measures"*. However, the Board considers that, while personnel making certification decisions may not have experience in *"significant professional experience in identifying and implementing data protection measures"* themselves, they should at least have access to someone with that expertise in order to make an informed decision. Significant professional experience in implementing such measures, at least in the early stages, would probably not be so widespread in this sector. Therefore, the Board encourages the UK SA to require that the certification body defines and explains the professional experience requirement which are appropriate to the certification scheme..

2.2.4 PROCESS REQUIREMENTS, ARTICLE 43(2)(C),(D) (Section 7 of the draft additional accreditation requirements)

17. Concerning the general subsection on process requirements (subsection 7.1) and, in particular, paragraph 4, the Board takes note of the additional requirement for an accreditation body to ensure that the certification body carries out an investigation or audit in cases where the data protection compliance is brought into question. The Board understands that the data protection compliance refers to the certification holder. However, this should be clearly specified in the requirements. Moreover, the Board considers that the UK SA should detail that such investigation should be linked with the scope of certification and the target of evaluation. Therefore, the Board recommends that the UK SA amends its requirement accordingly, by stating clearly that the data protection compliance refers to the certification holder and by specifying that the investigation should be linked with the scope of certification and the target of evaluation.

18. Concerning the application of process requirements (subsection 7.2), the Board takes note of the need for a certification body to specify "*whether processors are used, and when processors are the applicant, their responsibilities and tasks shall be described, and the application shall contain the relevant controller / processor contract(s).*" While acknowledging that the UK SA has used the wording

of Annex 1, the Board encourages the UK SA to consider whether a reference to joint controllers and their specific arrangements should also be mentioned in this case.

19. Concerning evaluation methods (subsection 7.4), the Board takes note of the additional requirement foreseen by the UK SA requiring that, "*In addition to item 7.4.5 of ISO17065, it shall be provided that existing certification, which relates to the same object of certification, may be taken into account as part of a new evaluation […]".* In this respect, the Board considers that it is necessary to further clarify that, in cases where existing certification is taken into account as part of a new evaluation, the scope of said certification should also be assessed in detail in respect of its compliance with the relevant certification criteria. Therefore, the Board encourages the UK SA to clarify the wording accordingly.

20. Concerning the sentence "*The complete evaluation report or information enabling an evaluation of the previous certification activity and its results can be considered.*" the Board recommends to the UK SA that "can" is replaced by "shall" where the certification body decides to take into account existing certification. In addition, the Board considers that it would be clearer to refer simply to "certification" rather than "certification activity" and recommends the UK SA to amend the draft accordingly. Moreover, the reference to the "previous certification" could be misleading, since it does not clearly refer to the existing certification the certification body wants to take into account as part of its own evaluation. The Board encourages the UK SA to change the wording, in order to clarify that the reference is to the existing certification. Finally, the Board notes that the certification body should be able to access the evaluation report and any other relevant information enabling an evaluation of the certification activity, in order to be able to take an informed decision. Therefore, the Board encourages the UK SA to clarify the wording accordingly.

21. Furthermore, in the paragraph starting with "*in addition to item 7.4.6 of ISO 17065*", the Board considers that, where the UK SA refers to "its certification mechanism", it actually meant "the certification scheme". Therefore, it recommends to the UK SA to replace the wording accordingly.

22. Regarding the changes affecting certification (subsection 7.10) and, in particular, the fourth bullet point ("decisions of the European Data Protection Board") the Board acknowledges that the UK SA has used the wording foreseen in Annex 1. However, in order to ensure a clear understanding of what is meant by "decisions of the European Data Protection Board", the Board encourages the UK SA to clarify the reference. An example could be to refer to "documents adopted by the European Data Protection Board".

3 CONCLUSIONS / RECOMMENDATIONS

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

24. Regarding 'general requirements for accreditation' the Board recommends that the UK SA:

    1. replaces, in subsection 4.1.1, the sentence "should be able to provide evidence" by "shall be able to provide evidence".

    2. includes in subsection 4.1.2 the missing part of the requirement, to align it with the text of the Annex 1 of the Guidelines.

25. Regarding 'process requirements' the Board recommends that the UK SA:

    1. amends subsection 7.1. in order to make clear that the data protection compliance refers to the certification holder and that the investigation should be linked with the scope of certification and the target of evaluation
    2. amends subsection 7.4 replacing "can" by "shall" and "certification activity" by "certification".
    3. replaces the reference to "certification mechanism" by "certification scheme".

4 FINAL REMARKS

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

27. According to Article 64 (7) and (8) GDPR, the supervisory authority 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.

For the European Data Protection Board

The Chair

(Andrea Jelinek)