Opinion 16/2020 on the draft decision of the competent supervisory authority of the Czech Republic 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 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 Czech Supervisory Authority (hereinafter "CZ SA") has submitted its draft accreditation requirements under Article 43 (1)(b) to the EDPB. The file was deemed complete on 17 February 2020. The CZ 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 CZ SA, once they are approved by the CZ 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 CZ SA has decided to resort to its national accreditation body (NAB) for the issuance of accreditation, having put together

[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

additional requirements in accordance with the Guidelines, which should be used by its NAB when issuing accreditation.

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

9. This opinion does not reflect upon items submitted by the CZ 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 the draft accreditation requirements do not completely follow the structure set out in Annex 1 to the Guidelines. For example, the sections on “scope” and “terms and definitions” are missing. In this regard, for the sake of clarity and to allow for an easier assessment of the requirements, the Board considers that the numbering and the overall structure of the document could be improved. Therefore, with the aim to facilitate the assessment, the Board encourages the CZ SA to follow the structure of the Annex in the draft accreditation requirements and add the missing sections, being of special relevance the definition of the terms used throughout the document. Moreover, the Board notes that the CZ SA’s draft accreditation requirements refer several times to the respective ISO 17065 section or to the respective sections of the Annex, without specifying however such reference. Thus, the Board encourages the CZ SA to make clear the references to the sections of the ISO 17065 and of the Annex.

13. The Board notes that the CZ SA's draft accreditation requirements refer several times to the "evaluated object" (e.g. sections 3.2.1.2.1.2.10; 3.2.1.2.6.3.1; 3.2.1.2.8.1.6.3; 3.2.1.2.10.4.1; 3.1.2.10.7.3.1; 3.1.2.10.7.3.2 and 3.2.1.2.10.10.2). The Board understands that this term is used as a synonym for the "target of evaluation". However, in order to ensure clarity, the Board encourages the CZ SA to use the term "target of evaluation" consistently.

14. The Board notes that several requirements are not formulated as an obligation of the certification body (e.g. 3.2.1.2.2 and 3.2.1.2.3). The Board encourages the CZ SA to redraft the requirements to make clear that they are mandatory -I.e. start the requirement with 'the certification body shall [...]".

2.2.3 GENERAL REQUIREMENTS FOR ACCREDITATION

15. Concerning the certification agreement (section 3.2.1.2.1.2 of the CZ SA's draft accreditation requirements), the Board notes that subsection 3.2.1.2.1.2.2 does not make any reference to the "contractually confidential matters", to which the SA shall also have access. Therefore, the Board recommends the CZ SA to amend the draft, by including the obligation to provide access to the SA to contractually confidential matters as well.

16. With regard to subsection 3.2.1.2.1.2.8 of the CZ SA's draft accreditation requirements, the Board notes that it is unclear as to whom the information shall be disclosed. Therefore, the Board encourages the CZ SA to clarify who will be the recipient of the information. Moreover, the information referred shall be "necessary for granting certification", as set out in section 4.1.2 point 7 of the Annex. The Board recommends the CZ SA to replace "information about granting certification" by "information necessary for granting certification".

17. Regarding subsection 3.2.1.2.1.2.9 of the CZ SA's draft accreditation requirements, it is unclear what type of information should be communicated directly to the Board. Article 42(8) GDPR sets out an obligation for the Board to collate, *inter alia*, all certification mechanisms. In this context, it is assumed that the competent SAs will provide the relevant information to the Board, who will then publish it on the public register. Therefore, the Board recommends the CZ SA to clarify subsection 3.2.1.2.1.2.9 of the draft requirements in line with Article 42(8) GDPR.

18. Concerning subsection 3.2.1.2.1.2.12 of the CZ SA's draft accreditation requirements, the Board takes note of the fact that the CZ SA created a reworded version of part of the requirement foreseen in the Annex. The CZ SA, however, omitted a reference to [where applicable] "the consequences for the customer should also be addressed". The Board therefore recommends the CZ SA to add the missing part of the requirement mentioned above.

19. Additionally, subsection 3.2.1.2.1.2.13 of the CZ SA's draft accreditation requirements establishes the obligation to "contain a commitment of the applicant to inform the certification body about all changes that may affect compliance of the certificated object with the certification criteria". The Board considers this formulation too generic, and recommends the CZ SA to amend the draft requirements in order to include "all changes in its actual or legal situation and in its products, processed and services concerned by the certification".

20. Concerning the use of data protection seals and marks (section 3.2.1.2.1.3 of the CZ SA's draft accreditation requirements), the Board notes that the CZ SA's draft requirements establish that the certification agreement shall contain "rules of using certificates, seals and marks if provided by the certification scheme owner". The same formulation is found in subsection 3.2.1.2.1.2.14. The Board considers that this obligation is already covered by item 4.1.2.2. letter l) of ISO 17065 and, therefore,

it should be contained in any certification scheme (see also item 4.1.3 of ISO 17065). Thus, for the sake of clarity, the Board recommends the CZ SA to delete the aforementioned sections.

21. With regard to the requirements on the management of impartiality, according to the information provided by the CZ SA in the template, section 4.2.1.b) and 4.2.2 of the Annex are sufficiently covered by item 4.2 of ISO 17065. However, the Board considers that these requirements shall be explicitly included in the draft accreditation requirements developed by the SAs in line with the Annex. Therefore, the Board recommends the CZ SA to include the missing requirements regarding the management of impartiality foreseen in the Annex.

22. With regard to the requirement on liability and financing (section 3.2.1.2.3.1 of the CZ SA's draft requirements), the Board encourages the CZ SA to specify that it has to be ensured on a regular basis.

2.2.4 RESOURCE REQUIREMENTS

23. Concerning certification body personnel (section 3.2.1.2.8.1.6 of the CZ SA's draft accreditation requirements), the Board notes that the requirements for personnel responsible for evaluations (subsection 3.2.1.2.8.1.6.3) include "*5-year practice with at least 10 performed audits carried out within certification activity in the same or similar field [...] or 5-year practice within certification of the objects of certification body focus)*". Similarly, the requirements for personnel responsible for decision-making (subsection 3.2.1.2.8.1.6.4) include "*at least 5-year practice with at least 10 performed audits carried out within certification activity in the same or similar field*". 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 CZ SA to redraft this subsection taking into account the different substantive knowledge and/or experience requirements for evaluators and decision-makers.

24. Furthermore, the Board takes note that point 3.2.1.2.9.1 of the CZ SA's draft accreditation requirements states that outsourcing is not allowed for certification activities. However, the following point allows the use of external auditors and external experts for evaluation, unless it constitutes certification activities. The Board considers that the draft accreditation requirements should specify when "it constitutes certification activities" or clarify that the certification body will retain the responsibility for the decision-making, even when it uses external experts. Therefore, the Board recommends the CZ SA to amend the draft accordingly.

2.2.5 PROCESS REQUIREMENTS

25. The Board notes that section 3.2.1.2.10.1.1 of the CZ SA's draft additional requirements refer to "all the additional requirements concerning a conflict of interests (7.1 point 1)". However, the CZ SA's draft additional requirements do not contain additional requirements concerning conflict of interest. Therefore, the Board encourages the CZ SA to amend the draft in order to avoid confusion.

26. With regard to the application requirements, the Board notes that subsection 3.2.1.2.10.2.3 of the CZ SA's draft accreditation requirements seems to imply that information on the transferred data shall only be provided in the application when the transfer is to a third country or international

organisation. However, the Board underlines that the applicant shall always contain a description of the data transferred to other systems or organisations, regardless of their location. Therefore, the Board encourages the CZ SA to amend the wording in order to avoid confusion.

27. The Board notes that the obligation to lay down in the certification agreement the binding evaluation methods (section 3.2.1.2.1.2.6 of the CZ SA's draft accreditation requirements) does not contain a reference to the Target of Evaluation, as per item 1 section 7.3 of the Annex to the Guidelines. For clarity purposes, the Board encourages the CZ SA to include such reference.

28. Moreover, the Board notes that CZ SA's draft accreditation requirements foresee the situation in which processors are used to carry out data processing operations, in line with the Annex to the Guidelines (section 3.2.1.2.10.2 of the CZ SA's draft accreditation requirements). The Board encourages the CZ SA to consider whether a reference to joint controllers and their specific arrangements should also be mentioned in this case.

29. Regarding the evaluation requirements (section 3.2.1.2.10.4 of the CZ SA's draft requirements), the Board notes that the CZ SA's accreditation requirements do not contain the obligation of the certification body to set out in detail in its certification mechanism how the information required in item 7.4.6 ISO 17065 shall be provided to the applicant about non conformities from a certification mechanism. As set out in the Annex (subsection 7.4), at least the nature and timing of such information shall be defined. Therefore, the Board recommends the CZ SA to add the aforementioned obligation.

30. Moreover, subsection 3.2.1.2.10.4.2 of the CZ SA's draft requirements seems to limit the evaluation methods to testing, auditing or inspections. The Board considers that other evaluation methods could also be used and, therefore, it encourages the CZ SA to amend the draft in order to make clear that the enumeration is not exhaustive.

31. Concerning subsection 3.2.1.2.10.4.4.1.4 of the CZ SA's draft accreditation requirements, the Board considers that the requirements should clearly state that the certification body is obliged to check the compliance with the criteria, and encourages the CZ SA to amend the draft accordingly.

32. With regard to the review requirements (subsection 3.2.1.2.10.5 of the CZ SA's draft accreditation requirements), the Board observes that the CZ SA's draft accreditation requirements do not make reference to the obligation to set out procedures for the granting and revocation of certifications. The Board recommends the CZ SA to amend the draft accordingly.

33. Concerning the requirements on certification documentation, the Board notes that section 3.1.2.10.7.2 of the CZ SA's draft accreditation requirements states that the certification body shall specify that monitoring is a condition of validity of certification "if monitoring required by a certification scheme [...]". The Board considers that, in the case of certification under the GDPR, the monitoring activities are always mandatory and, therefore, recommends the CZ SA to include such obligation.

34. With regard to the requirements related to the directory of certified products (section 3.2.1.2.10.8 of the CZ SA's draft accreditation requirements and 7.8 of the Annex), and particularly, the obligation to inform the competent SA of the reasons for granting or revoking the requested certification, the Board notes that the CZ SA's draft accreditation requirements refer to section 3.2.1.2.10.4.5. However, such section concerns the obligation to make the evaluation documentation accessible to the CZ SA upon request, whereas the requirement in section 7.8 of the Annex to the Guidelines contains an obligation

to proactively inform the SA of the reasons for granting or revoking the certification. Therefore, the Board recommends the CZ SA to amend the draft accordingly.

35. Regarding the changes affecting certification, the Board notes that the CZ SA's draft accreditation requirements do not mention, among the procedures to be agreed, the approval process with the competent SA, referenced in the Annex to the Guidelines (page 19). The Board acknowledges that the list provided in section 7.10 of the Annex is not mandatory. However, in order to ensure consistency, the Board encourages the CZ SA to add a reference to the approval process with the SA.

36. The Board observes that the CZ SA's draft accreditation requirements do not clearly include the obligation of the certification body to accept decisions and orders from the competent SA to withdraw or not to issue certification to an applicant if the requirements for certification are no longer met. The Board recommends the CZ SA to clearly include such obligation in the draft accreditation requirements. With regard to the termination, reduction, suspension or withdrawal of certification, the Board notes that sections 3.2.1.2.10.10.2 and 3.2.1.2.10.10.3 of the draft requirements refer to an "instigation". If the intention is to refer to "decisions and orders" from the SA, as established in article 58(2)(h) GDPR, the Board encourages the CZ SA to use the same terminology as the GDPR, and refer to "decisions and orders".

2.2.6 MANAGEMENT SYSTEM

37. The Board considers that section 3.2.1.2.11 of the CZ SA's draft additional requirements do not contain the obligation of the certification body to "make public permanently and continuously which certifications were carried out on which basis, how long the certifications are valid under which framework and conditions", as stated in section 8 of the Annex. Therefore, the Board recommends the CZ SA to amend the draft requirements by including the abovementioned reference.

3 CONCLUSIONS / RECOMMENDATIONS

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

39. Regarding 'general requirements for accreditation', the Board recommends that the CZ SA:

1) include the obligation to provide access to the SA to "contractually confidential matters" in section 3.2.1.2.1.2.

2) replace "information about granting certification" with "information necessary for granting certification" in subsection 3.2.1.2.1.2.8.

3) clarify subsection 3.2.1.2.1.2.9 in line with Article 42(8) GDPR.

4) in subsection 3.2.1.2.1.2.12, add a reference to [where applicable] "the consequences for the customer should also be addressed".

5) amend subsection 3.2.1.2.1.2.13 to include "all changes in its actual or legal situation and in its products, processed and services concerned by the certification".

6) delete section 3.2.1.2.1.3 and subsection 3.2.1.2.1.2.14.

7) include the missing requirements regarding the management of impartiality foreseen in the Annex.

40. Regarding 'resource requirements', the Board recommends that the CZ SA:

1) amend section 3.2.1.2.9.1 to specify when "it constitutes certification activities" or clarify that the certification body will retain the responsibility for the decision-making, even when it uses external experts.

41. Regarding 'process requirements', the Board recommends that the CZ SA:

1) include, in section 3.2.1.2.10.4, the obligation of the certification body to set out in detail in its certification mechanism how the information required in item 7.4.6 ISO 17065 shall be provided to the applicant about non conformities from a certification mechanism.

2) amend section 3.2.1.2.10.5 to make reference to the obligation to set out procedures for the granting and revocation of certifications.

3) amend section 3.1.2.10.7.2 to reflect that in the case of certification under the GDPR, the monitoring activities are always mandatory.

4) amend section 3.2.1.2.10.8 to reflect the obligation of the certification body to proactively inform the SA of the reasons for granting or revoking the certification.

5) include the obligation of the certification body to accept decisions and orders from the competent SA to withdraw or not to issue certification to an applicant if the requirements for certification are no longer met.

42. Regarding 'management system', the Board recommends that the CZ SA:

1) include the obligation of the certification body to "make public permanently and continuously which certifications were carried out on which basis, how long the certifications are valid under which framework and conditions", as stated in section 8 of the Annex.

4 FINAL REMARKS

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

44. According to Article 64 (7) and (8) GDPR, the CZ 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.

45. The CZ 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