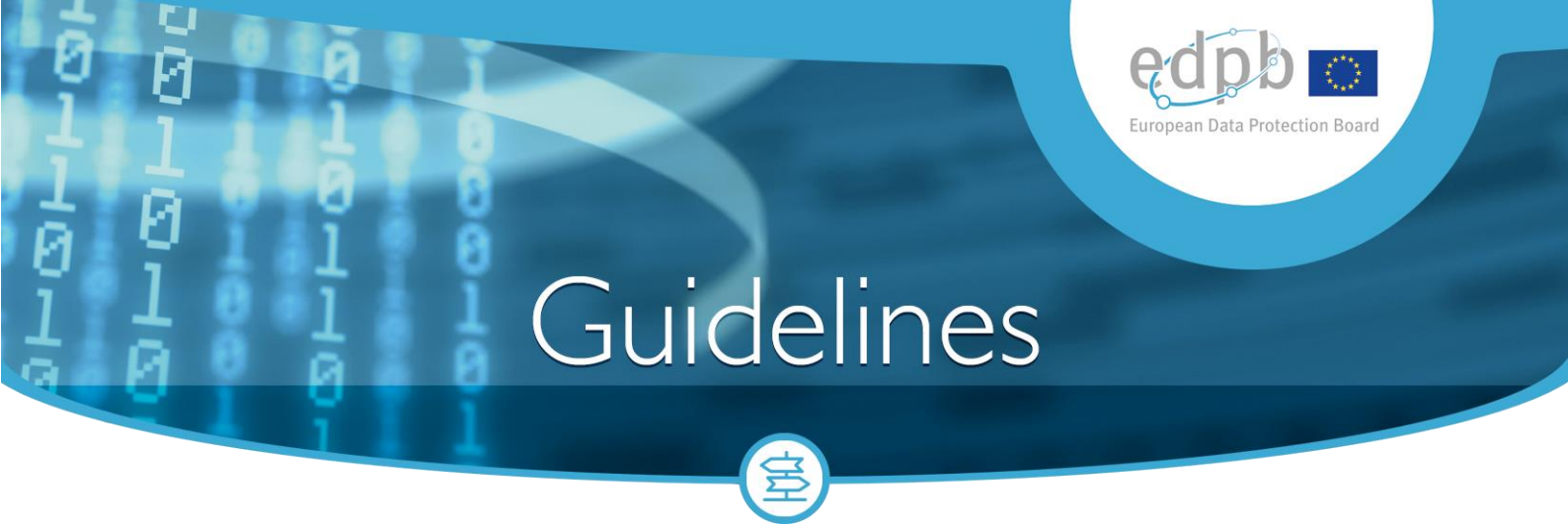

Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679) - Annex 1

Version for public consultation

Adopted on 4 December 2018

Contents

ANNEX 1

Annex 1 provides guidance for the specification of "additional" accreditation requirements with respect to ISO/IEC 17065/2012 and in accordance with Articles 43(1)(b) and 43(3) GDPR.

This sets out suggested requirements that a data protection supervisory authority shall draft and that apply during the accreditation of a certification body for a certification mechanism with supervisory authority or European Data Protection Board (EDPB) approved criteria. These additional requirements are to be communicated to the European Data Protection Board before approval pursuant to Article 64(1)(c).

This annex should be read in conjunction with ISO/IEC 17065/2012. Section numbers used here correspond to those used in ISO/IEC 17065/2012.

The absence of comments on any item does not mean that no further additional requirements can be formulated by the supervisory authority concerning these items if in accordance with the national law.

0 PREFIX

[This section is for any agreed Terms of cooperation, if applicable, between National Accreditation Body and the data protection supervisory authority, e.g. who should be responsible to receive applications.]

1 SCOPE[1]

The scope of ISO/IEC 17065/2012 shall be applied in accordance with the GDPR. The guidelines on accreditation and certification provide guidance. Any concretisation of the scope should be taken into account in the assessment by the NAB during the accreditation process, particularly with respect to criteria, expertise and evaluation methodology. It should not lead to a lowering of the requirements of the GDPR. Pursuant to Article 42(1), certification is applicable to the processing operations of controllers and processors.

2 NORMATIVE REFERENCE

GDPR has precedence over ISO/IEC 17065/2012. If, in the additional requirements or by certification mechanism, reference is made to other ISO norms, they shall be interpreted in line with the requirements set out in the GDPR.

3 TERMS AND DEFINITIONS

In the context of this Annex, the terms and definitions of the guidelines on accreditation (WP 261) and certification (EDPB 1/2018) shall apply and have precedence over ISO definitions.

[1] Numbering refers to ISO/IEC 17065/2012.

4 GENERAL REQUIREMENTS FOR ACCREDITATION

4.1 Legal and contractual matters

4.1.1 Legal responsibility and accountability

In addition to the legal responsibility of a certification body, accreditation shall ensure that a certification body is at all times able to demonstrate compliance with the terms of accreditation and its application of Regulation 2016/679/EC to applicant organisations and in respect of its own data controller obligations.

4.1.2 Certification agreement ("CA")

The minimum requirements for a certification agreement shall be supplemented by the following points:

The certification body shall demonstrate in addition to the requirements of ISO/IEC 17065/2012 that its certification agreements:

1. require the applicant to always comply with both the general certification requirements within the meaning of 4.1.2.2 lit. a ISO/IEC 17065/2012 and the criteria approved by the competent supervisory authority or the EDPB in accordance with Article 43 (2)(b) and Article 42(5);
2. require the applicant to allow full transparency to the competent supervisory authority with respect to the certification procedure including contractually confidential matters related to data protection compliance pursuant to Articles 42(7) and 58(1)(c);
3. do not reduce the responsibility of the applicant for compliance with Regulation 2016/679/EC and is without prejudice to the tasks and powers of the supervisory authorities which is competent in line with Article 42(5);
4. require the applicant to provide the certification body with all information and access to its processing activities which are necessary to conduct the certification procedure pursuant to Article 42(6);
5. require the applicant to comply with applicable deadlines and procedures. The certification agreement must stipulate that deadlines and procedures resulting, for example, from the certification program or other regulations must be observed and adhered to;
6. with respect to 4.1.2.2 lit. c No. 1 ISO/IEC17065/2012 set out the rules of validity, renewal, and withdrawal pursuant to Articles 42(7), 43(4) including rules setting appropriate intervals for re-evaluation or review (regularity) in line with Article 42(7);
7. allow the certification body to disclose all information necessary for granting certification pursuant to Articles 42(8), 43(5);
8. include rules on the necessary precautions for the investigation of complaints within the meaning of 4.1.2.2 lit. c No. 2, additionally, lit. j, shall also contain explicit statements on the structure and the procedure for complaint management in accordance with Article. 43(2)(d)
9. in addition to the minimum requirements referred to in 4.1.2.2 EN-ISO-17065/2012, the consequences of withdrawal of accreditation for the certification body and its customers (applicants and seal holders) shall also be regulated as the certification of the customer is dependent on the accreditation of the certification body

10. require the applicant to inform the certification body in the event of significant changes in its actual or legal situation and in its products, processes and services concerned by the certification.

4.1.3 Use of data protection seals and marks

Certificates, seals and marks shall only be used in compliance with Article 42 and 43 and the guidelines on accreditation and certification.

4.2 Management of impartiality

The accreditation body shall ensure that in addition to the requirement in 4.2. ISO/IEC 17065/2012

1. the certification body comply with the additional requirements of the competent supervisory authority (pursuant to Article 43(1)(b))
    a. in line with Article 43(2)(a) separate evidence of its independence. This applies in particular to evidence concerning the financing of the certification body in so far as it concerns the assurance of impartiality;
    b. its tasks and obligations do not lead to a conflict of interest pursuant to Article 43(2)(e);
2. the certification body has no relevant connection with the body it assesses.

4.3 Liability and financing

The accreditation body shall in addition to the requirement in 4.3.1 ISO/IEC 17065/2012 ensure on a regular yearly basis that the certification body has appropriate measures (e.g. insurance or reserves) to cover its liabilities in the geographical regions in which it operates.

4.4 Non-discriminatory conditions

Additional requirements may be formulated by the supervisory authority if in accordance with the national law.

4.5 Confidentiality

Additional requirements may be formulated by the supervisory authority if in accordance with the national law.

4.6 Publicly available information

The accreditation body shall in addition to the requirement in 4.6 ISO/IEC 17065/2012 require from the certification body that

1. all versions of the approved criteria used within the meaning of Article 42(5) are published and easily publicly available as well as all the certification procedures used, generally stating the respective period of validity;
2. information about procedures handling complaints an appeals are made public pursuant to Article 43(2)(d).

5 STRUCTURAL REQUIREMENTS, ARTICLE 43(4) ["PROPER" ASSESSMENT]

5.1 Organisational structure and top management

Additional requirements may be formulated by the supervisory authority.

5.2 Mechanisms for safeguarding impartiality

Additional requirements may be formulated by the supervisory authority.

6 RESOURCE REQUIREMENTS

6.1 Certification body personnel

The accreditation body shall in addition to the requirement in section 6 EN-ISO-17065/2012 ensure for each certification body that its personnel:

1. has demonstrated appropriate and ongoing expertise (knowledge and experience) with regard to data protection pursuant to Article 43(1);
2. has independence and ongoing expertise with regard to the object of certification pursuant to Article 43(2)(a) and do not have a conflict of interest pursuant to Article 43(2)(e);
3. undertakes to respect the criteria referred to in Article 42(5) pursuant to Article 43(2)(b);
4. has relevant and appropriate knowledge about and experience in applying data protection legislation;
5. has relevant and appropriate knowledge about and experience in technical and organisational data protection measures as relevant.
6. is able to demonstrate experience in the fields mentioned in the additional requirements 6.1.1, 6.1.4, and 6.1.5, specifically

For personnel with technical expertise:

- Have obtained a qualification in a relevant area of technical expertise to at least EQF[2] level 6 or a recognised protected title in the relevant regulated profession or have significant professional experience.
- *Personnel responsible for certification decisions* require significant professional experience in identifying and implementing data protection measures.
- *Personnel responsible for evaluations* require professional experience in technical data protection and knowledge and experience in comparable procedure (e.g. certifications/audits), and registered as applicable.
    - Personnel shall demonstrate they keep current domain specific knowledge in technical and audit skills through continuous professional development.

For personnel with legal expertise:

- Legal studies at an EU or state-recognised university for at least eight semesters including the academic degree Master (LL.M.) or equivalent or equivalent or significant professional experience.
- *Personnel responsible for certification decisions* shall demonstrate significant professional experience in data protection law and be registered as required by the Member State.
- *Personnel responsible for evaluations* shall demonstrate at least two years of professional experience in data protection law and knowledge and experience in

[2] See qualification framework comparison tool at https://ec.europa.eu/ploteus/en/compare?

comparable procedures (e.g. certifications/audits), and registered as required by the Member State.

- Personnel shall demonstrate they keep current domain specific knowledge in technical and audit skills through continuous professional development.

6.2 Resources for evaluation

Additional requirements may be formulated by the supervisory authority if in accordance with the national law.

7 PROCESS REQUIREMENTS, ARTICLE 43(2)(C),(D)

7.1 General

The accreditation body shall in addition to the requirement in section 7.1 EN-ISO-17065/2012 be required to ensure the following:

1. Certification bodies comply with the additional requirements of the competent supervisory authority (pursuant to Article 43(1)(b)) when submitting the application that tasks and obligations do not lead to a conflict of interests pursuant to Article 43(2)(b);
2. Certification bodies are controllers and processors with respect to their processing activities and are eligible for application pursuant to Article 42(7).

7.2 Application

In addition to item 7.2 of ISO/IEC 17065, it should be required that

1. the object of certification (ToE) must be described in detail in the application. This also includes interfaces and transfers to other systems and organizations, protocols and other assurances;
2. the application shall 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 contract(s) binding the controller and the processors.

7.3 Application Review

In addition to item 7.3 of ISO/IEC 17065, it should be required that

1. binding evaluation methods with respect to the ToE shall be laid down in the certification agreement;
2. the assessment in 7.3(e) of whether there is sufficient expertise takes into account both technical and legal expertise in data protection to an appropriate extent.

7.4 Evaluation

In addition to item 7.4 of ISO/IEC 17065, certification mechanisms shall describe sufficient evaluation methods for assessing the compliance of the processing operation(s) with the certification criteria, including for example where applicable:

1. a method for assessing the necessity and proportionality of processing operations in relation to their purpose and the data subjects concerned;
2. a method for assessing the coverage, composition and assessment of all risks considered by controller and processor with regard to the legal consequences pursuant to Articles 30, 32 and 35 and 36 GDPR, and with regard to the definition of technical and organisational measures

pursuant to Articles 24, 25 and 32 GDPR, insofar as the aforementioned norms apply to the object of certification, and

3. a method for assessing the remedies, including guarantees, safeguards and procedures to ensure the protection of personal data in the context of the processing to be attributed to the object of certification and to demonstrate that the legal requirements are met; and
4. documentation of methods and findings.

The certification body should be required to ensure that these evaluation methods are general and standardized. This means that comparable evaluation methods are used for comparable ToEs. Any deviation from this procedure must be justified by the certification body.

In addition to item 7.4.2 of ISO/IEC 17065, it should be required that the evaluation may be carried out by external experts who have been recognized by the certification body

In addition to item 7.4.5 of ISO/IEC 17065, it should be required that data protection certification in accordance with Articles 42 and 43 GDPR, which already covers part of the object of certification, may be included in a current certification. However, it will not be sufficient to completely replace (partial) evaluations. The certification body shall be obliged to check the compliance with the criteria. Recognition shall in any way require the availability of a complete evaluation report or information enabling an evaluation of the previous certification activity and its results. A certification statement or similar certification certificates should not be considered sufficient to replace a report.

In addition to item 7.4.6 of ISO/IEC 17065, it should be required that the certification body shall set out in detail in its certification criteria how the information required in item 7.4.6 informs the customer (certification applicant) about deviations from a certification mechanism. In this context, at least the nature and timing of such information should be defined.

In addition to item 7.4.9 of ISO/IEC 17065, it should be required that documentation be made fully accessible to the data protection supervisory authority upon request.

7.5 Review

In addition to item 7.5 of ISO/IEC 17065, procedures for the granting, regular review and revocation of the respective certifications pursuant to Article 43(2) and 43(3) to be in place should be required.

7.6 Certification decision

In addition to point 7.6.1 of ISO/IEC 17065, the certification body should be required to set out in detail in its criteria how its independence and responsibility with regard to individual certification decisions are ensured.

7.7 Certification documentation

In addition to item 7.7.1.e of ISO/IEC 17065 and in accordance with Article 42(7) GDPR, it should be required that the period of validity of certifications shall not exceed three years.

In addition to item 7.7.1.e of ISO/IEC 17065, it should be required that the period of the intended monitoring within the meaning of section 7.9 will also be documented.

In addition to item 7.7.1.f of ISO/IEC 17065, the certification body should be required to name the object of certification in the certification documentation (stating the version status or similar characteristics, if applicable).

7.8 Certification documentation

In addition to item 7.8 of ISO/IEC 17065, the certification body should be required to keep the information on certified products, processes and services available internally and publicly available. The information should provide:

(a) a short version of the evaluation report regarding the respective certification result, from which the object of certification (including version or functional status) can be understood,

(b) the evaluation methods and tests (including the criteria on which the certification is based (if applicable with version information)) and

(c) the test result(s).

In addition to item 7.8 of ISO/IEC 17065 and pursuant to Article 43(5) GDPR, the certification bodies shall inform the competent supervisory authorities of the reasons for granting or revoking the requested certification.

7.9 Surveillance

In addition to points 7.9.1, 7.9.2 and 7.9.3 of ISO/IEC 17065, and according to Article 43(2)(c) GDPR, it should be required that regular monitoring measures are obligatory to maintain certification during the monitoring period.

7.10 Changes affecting certification

In addition to points 7.10.1 and 7.10.2 of DIN EN ISO/IEC 17065, the certification body should be required to define processes in its certification programme to ensure that the customer (applicant or seal holder) is promptly informed of changes in the legal framework resulting from amendments to the law, the adoption of delegated acts of the European Commission in accordance with 43(8) and 43(9), decisions of the European Data Protection Committee and court decisions, and developments in the state of the art relevant to its certifications and monitoring. This includes measures and procedures to revoke the certification if the certified processing operation is no longer in compliance with the updated criteria which were revised due to the aforementioned changes.

7.11 Termination, reduction, suspension or withdrawal of certification

In addition to chapter 7.11.1 of ISO/IEC 17065, the certification body should be required to inform the competent supervisory authority immediately in writing about measures taken and about continuation, restrictions, suspension and withdrawal of certification.

According to Article 58(2)(h), the certification body shall be required to accept decisions and orders from the competent supervisory authority to withdraw or not to issue certification to a customer (applicant) if the requirement for certification are not or no longer met.

7.12 Records

The Certification Body should be required to keep all documentation complete, comprehensible, up-to-date and fit to audit.

7.13 Complaints and appeals, Article 43(2)(d)

In addition to item 7.13.1 of ISO/IEC 17065, the certification body should be required to define,

(a) who can file complaints or objections,
(b) who processes them on the part of the certification body,
(c) which verifications take place in this context; and
(d) the possibilities for consultation of interested parties.

Adopted

In addition to item 7.13.2 of ISO/IEC 17065, the certification body should be required to define,

(a) how and to whom such confirmation must be given,
(b) the time limits for this; and
(c) which processes are to be initiated afterwards.

In addition to item 7.13.1 of ISO/IEC 17065, the certification body must define how separation between certification activities and the handling of appeals and complaints is ensured.

8 MANAGEMENT SYSTEM REQUIREMENTS

A general requirement of the management system according to chapter 8 of ISO/IEC 17065 is that the implementation of all requirements from the previous chapters within the scope of the application of the certification mechanism by the accredited certification body is documented, evaluated, controlled and monitored independently.

The basic principle of management is to define a system according to which its goals are set effectively and efficiently, specifically: the implementation of the certification services - by means of suitable specifications. This requires transparency and verifiability of the implementation of the accreditation requirements by the certification body and its permanent compliance.

To this end, the management system must specify a methodology for achieving and controlling these requirements in compliance with data protection regulations and for continuously checking them at with the accredited body itself.

These management principles and their documented implementation must be transparent and be disclosed by the accredited certification body pursuant in the accreditation procedure pursuant to Article 58 and thereafter at the request of the data protection supervisory authority at any time during an investigation in the form of data protection reviews pursuant to Art. 58(1)(b) or a review of the certifications issued in accordance with Article 42(7) pursuant to Article 58(1)(c).

In particular, the accredited certification body must make public permanently and continuously which certifications were carried out on which basis (or certification mechanisms or schemes), how long the certifications are valid under which framework and conditions (recital 100).

8.1 General management system requirements

The competent supervisory authority may specify and add further additional requirements if in accordance with the national law.

8.2 Management system documentation

The competent supervisory authority may specify and add further additional requirements if in accordance with the national law.

8.3 Control of documents

The competent supervisory authority may specify and add further additional requirements if in accordance with the national law.

8.4 Control of records

The competent supervisory authority may specify and add further additional requirements if in accordance with the national law.

8.5 Management Review

The competent supervisory authority may specify and add further additional requirements if in accordance with the national law.

8.6 Internal audits

The competent supervisory authority may specify and add further additional requirements if in accordance with the national law.

8.7 Corrective actions

The competent supervisory authority may specify and add further additional requirements if in accordance with the national law.

8.8 Preventive actions

The competent supervisory authority may specify and add further additional requirements if in accordance with the national law.

9 FURTHER ADDITIONAL REQUIREMENTS[3]

9.1 Updating of evaluation methods

The certification body shall establish procedures to guide the updating of evaluation methods for application in the context of the evaluation under point 7.4. The update must take place in the course of changes in the legal framework, the relevant risk(s), the state of the art and the implementation costs of technical and organisational measures.

9.2 Maintaining expertise

Certification bodies shall establish procedures to ensure the training of their employees with a view to updating their skills, taking into account the developments listed in point 8.9.2.

9.3 Responsibilities and competencies

9.3.1 Communication between CB and its customers

Procedures shall be in place for implementing appropriate procedures and communication structures between the certification body and its customer. This shall include

1. Maintaining documentation of tasks and responsibilities by the accredited certification body, for the purpose of
    a. Information requests, or
    b. To enable contact in the event of a complaint about a certification.
2. Maintaining an application process for the purpose of
    a. Information on the status of an application;
    b. Evaluations by the competent supervisory authority with respect to
        i. Feedback;
        ii. Decisions by the competent supervisory authority.

[3] The competent supervisory authority may specify and add further additional requirements if in accordance with national law.

9.3.2 Documentation of evaluation activities

Additional requirements may be formulated by the supervisory authority.

9.3.3 Management of complaint handling

A complaint handling shall be established as an integral part of the management system, which shall in particular implement the requirements of points 4.1.2.2 lit. c), 4.1.2.2 lit. j), 4.6 lit. d) and 7.13 ISO/IEC 17065.

Relevant complaint and objections should be shared with the competent supervisory authority.

9.3.4 Management of withdrawal

The procedures in the event of suspension or withdrawal of the accreditation shall be integrated into the management system of the certification body including notifications of customers.

For the European Data Protection Board

The Chair

(Andrea Jelinek)