The Norwegian Data Protection Authority's Additional Accreditation Requirements for Certification Bodies

February 2024

Datatilsynet

The Norwegian Data Protection Authority

Table of Contents

Introduction

This document provides the Norwegian Supervisory Authority's (the Norwegian SA) additional accreditation requirements with respect to ISO/IEC 17065:2012 (hereinafter ISO 17065) and in accordance with Articles 43 (1) (b) and 43 (3) of the GDPR. The sections below (aside from section 9) refer to ISO 17065 section headings and set out the additional requirements for the relevant ISO 17065 section numbers.

Prefix

According to Article 43 (1) (a) and (b) in the GDPR, the Norwegian SA and Norwegian Accreditation (NA) as Norway's National Accreditation Body (NAB), are both empowered to grant accreditation to certification bodies.

However, in practice, NA will be responsible for accrediting certification bodies, as NA has extensive experience in accreditation in other areas. Therefore, a company (or a public authority) must contact NA if it wants to be accredited as a certification body.

The terms of cooperation between the Norwegian SA and NA are set out in a cooperation agreement drafted by NA and the Norwegian SA. The cooperation agreement sets out the roles, responsibilities and operational procedures in relation to accreditation for GDPR certification schemes. The cooperation agreement is available on the Norwegian SA's website.

If at some point the Norwegian SA chooses to use its powers to grant accreditation in accordance with Article 43 (1) (a) GDPR, the Norwegian SA will accredit certification bodies in accordance with ISO 17065 and these additional requirements with the necessary adjustments. The necessary adjustments will primarily consist of referring to the Norwegian SA where the additional requirements now refer to the NAB.

1 Scope

This document contains additional requirements to ISO 17065 for assessing the competence, consistent operation and impartiality of GDPR certification bodies.

The scope of ISO 17065 shall be applied in accordance with the GDPR. The European Data Protection Board's (EDPB) guidelines on accreditation[1] and certification[2] provide further information.

The broad scope of ISO 17065 covering products, processes and services does not lower or override the requirements of the GDPR. Therefore, certification must be in respect of personal data processing operations. Whilst a governance system, for example a privacy information management system, can form part of a certification mechanism, it cannot be the only element of a certification mechanism, as the certification must include processing of personal data.

The scope of a certification mechanism (for example, certification of cloud service processing operations) shall be taken into account in the assessment by the accreditation body during the accreditation process, particularly with respect to criteria, expertise and evaluation methodology.

Finally, pursuant to Article 42(1) of the GDPR, GDPR certification can only be awarded in relation to controllers and processors' processing operations.

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

[2] Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation

2 Normative references

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

3 Terms and definitions

The terms and definitions of the EDPB Accreditation Guidelines and EDPB Certification Guidelines (as defined below) shall apply and have precedence over ISO definitions. For ease of reference, the main definitions used in this document are listed below.

Accreditation: An attestation by a national accreditation body and/or by a supervisory authority, that a certification body is qualified to carry out certification pursuant to Article 42 and 43 of the GDPR, taking into account ISO 17065 and the additional requirements established by the supervisory authority and/or by the EDPB. For further information on the interpretation of accreditation for the purposes of Article 43 of the GDPR, see section 3 of the EDPB Accreditation Guidelines.

Accreditation body: Body that performs accreditation. In this document, this term is taken to mean NA. If at some point, the Norwegian SA chooses to use its empowerment to grant accreditation, the term is taken to mean the Norwegian SA.

Applicant: The organisation that has applied to have their processing operations certified, usually a data controller carrying out data processing or a data processor offering evaluated products and services associated with data processing.

Certification: The assessment and impartial third-party attestation that fulfilment of the certification criteria has been demonstrated in respect of a controller or processor's processing operations.

Certification body: Third party conformity assessment body operating certification schemes.

Certification criteria: The criteria against which an organisation's processing operations are measured for a given certification scheme.

Certification mechanism: An approved certification scheme, which is available to the applicant. It is a service provided by an accredited certification body based on approved criteria and assessment methodology. It is the system by which a controller or processor becomes certified.

Certification scheme: A certification system related to specified products, processes and services to which the same specified requirements, specific rules and procedures apply. It includes the certification criteria and assessment methodology.

Client:[3] The organisation that has been certified (previously the applicant).

Competent supervisory authority: Where referred to in this document, this means the Norwegian SA.

CSA: A supervisory authority concerned, as defined in Article 4 (22) of the GDPR.

[3] Whenever the term "client" is used in the International Standard (ISO/IEC 17065/2012), it applies to both the "applicant" and the "client", unless otherwise specified.

EDPB Accreditation Guidelines: EDPB Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the GDPR (2016/679).

EDPB Certification Guidelines: EDPB Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the GDPR.

Evaluation: The activity of the certification body consisting of an assessment of whether the Target of Evaluation complies with the approved certification criteria.

General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 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.

ISO 17065: ISO/IEC 17065:2012.

National accreditation body (NAB): the sole body in a Member State named in accordance with Regulation (EC) No 765/2008 of the European Parliament and the Council that performs accreditation with authority derived from the State. In Norway, Norwegian Accreditation (NA) is the NAB.

PDA18: The Norwegian Personal Data Act 2018 (Act No. 38 of 15 June 2018 as amended).

Target of Evaluation or ToE: The object of certification. In the case of GDPR certification, this will be the relevant processing operation(s) that the controller or processor is applying to have evaluated and certified.

4 General requirements for accreditation

4.1 Legal and contractual matters

4.1.1 Legal responsibility

A certification body shall be able to demonstrate (at all times) to the accreditation body that they have up to date procedures that demonstrate compliance with the legal responsibilities set out in the terms of accreditation, including the additional requirements in respect of the application of the GDPR.

The certification body shall be able to demonstrate that its procedures and measures specifically for controlling and handling of applicant and client organisation's personal data as part of the certification process are compliant with the GDPR and the PDA18. As such, it shall provide evidence of compliance as required during the accreditation process.

This shall include the certification body confirming to the accreditation body that they are not the subject of any investigation – and have not previously been the subject of any regulatory action – by the Norwegian SA under the GDPR or PDA18, which may entail that they do not meet the aforementioned requirement and therefore might prevent their accreditation. Before proceeding with the accreditation process, the accreditation body may contact the Norwegian SA in order to verify this information. The Norwegian SA will verify the information where appropriate.

The certification body shall also confirm to the accreditation body that they are not the subject of any investigation – and have not previously been the subject of any regulatory actions by other supervisory authorities within other sectors, if these investigations or regulatory actions concern processing of personal data and may result in the certification body not meeting the aforementioned requirement, and therefore might prevent their accreditation.

The certification body shall inform the accreditation body immediately of relevant infringements of GDPR or the PDA18 established by the Norwegian SA, supervisory authorities within other sectors or competent judicial authorities that may affect its accreditation.

Prior to issuing or renewing a certification, the certification body shall be required to notify the Norwegian SA pursuant to Article 43 (1) of the GDPR.

The Norwegian SA may decide to add further requirements and procedures to check certification bodies' GDPR compliance prior to accreditation.

4.1.2 Certification agreement

The certification body shall demonstrate, in addition to the requirements of section 4.1.2.1 of ISO 17065, that its certification agreements:

1. require the applicant to always comply with both the general certification requirements within the meaning of section 4.1.2.2 (a) of ISO 17065 and the criteria approved by the Norwegian SA or the EDPB in accordance with Article 43 (2) (b) and Article 42 (5) of the GDPR;

2. require the applicant to allow full transparency to the Norwegian SA with respect to the certification procedure including any confidential materials, whether contractual or imposed by the law, related to data protection compliance pursuant to Articles 42 (7) and 58 (1) (c) of the GDPR;
3. do not reduce the responsibility of the applicant for compliance with the GDPR and is without prejudice to the tasks and powers of the supervisory authorities which are competent in line with Article 42 (5) of the GDPR;
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) of the GDPR;
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 section 4.1.2.2 (c) (1) of ISO 17065, set out the rules of validity, renewal, and withdrawal pursuant to Articles 42 (7) and 43 (4) of the GDPR, including rules setting appropriate intervals for re-evaluation or review (regularity) in line with Article 42 (7) of the GDPR and section 7.9 of these requirements;
7. allow the certification body to disclose to the Norwegian SA the reasons for granting or withdrawing the certification pursuant to Article 43 (5) of the GDPR, and the information that the Norwegian SA will need to provide to the EDPB in order to enable the EDPB to include the certification mechanism in a publicly available register pursuant to Article 42 (8) of the GDPR;
8. include rules on the necessary precautions for the investigation of complaints within the meaning of sections 4.1.2.2 (c) (2)and (j) of ISO 17065, in a transparent and easily accessible manner, which shall also contain explicit statements on the structure and the procedure for complaint management in accordance with Article 43 (2) (d) of the GDPR;
9. in addition to the minimum requirements referred to in section 4.1.2.2 of ISO 17065, the certification agreement shall contain an explanation of the consequences of withdrawal or suspension of accreditation for the certification body and how this impacts the client. In that case, the consequences for the client and any potential next steps that may be taken shall also be addressed by including appropriate procedures in the management system 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;
11. include binding evaluation methods with respect to the ToE; and
12. require the applicant to inform the certification body of any infringements of the GDPR established by the Norwegian SA and/or judicial authorities that may affect 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 of the GDPR, the EDPB Accreditation Guidelines and the EDPB Certification Guidelines.

4.2 Management of impartiality

The accreditation body shall ensure that, in addition to complying with the requirements in section 4.2 of ISO 17065:

1. the certification body shall comply with the additional requirements of the Norwegian SA (pursuant to Article 43 (1) (b) of the GDPR):
    a. in line with Article 43 (2) (a) of the GDPR, provide 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; and
    b. have clear rules in place for identifying and managing potential conflicts of interest, and ensure its tasks and obligations do not lead to a conflict of interest pursuant to Article 43 (2) (e) of the GDPR;
2. the certification body has no relevant connection with the client it assesses. For example:
    a. Any type of economic relation between the certification body and the client, depending on its features, may affect the impartiality of the certification body's certification activities.
    b. The certification body may not belong to the same company group/legal entity as the client it assesses.
    c. The certification body may not be controlled in any way by the client it assesses.
    d. The certification body may not be in a controller/processor relationship with the client it assesses.

4.3 Liability and financing

In addition to the requirements in section 4.3.1 of ISO 17065, the certification body shall demonstrate to the accreditation body on a regular basis (i.e. once a year) that it has appropriate measures (e.g. insurance and/or reserves) to cover its liabilities in the geographical regions in which it operates.

Furthermore, the certification body shall demonstrate its financial stability and independence. The decision with respect to the selection and designation of the supporting documents lies within the discretion of the accreditation body.

4.4 Non-discriminatory conditions

The requirements in section 4.4 of ISO 17065 shall apply.

4.5 Confidentiality

The requirements in section 4.5 of ISO 17065 shall apply.

4.6 Publicly available information

In addition to the requirements in section 4.6 of ISO 17065, the accreditation body shall, as a minimum, require from the certification body that:

1. all versions (current and previous) of the approved criteria used within the meaning of Article 42 (5) of the GDPR are published and easily publicly available as well as all certification procedures, generally stating the respective period of validity; including, where applicable, that the criteria have been approved by the EDPB; and

2. information about complaints handling procedures and appeals are made public pursuant to Article 43 (2) (d) of the GDPR.

5 Structural Requirements, Article 43 (4) of the GDPR [“Proper” Assessment]

5.1 Organisational structure and top management

The requirements in section 5.1 of ISO 17065 shall apply.

5.2 Mechanisms for safeguarding impartiality

The requirements in section 5.2 of ISO 17065 shall apply.

6 Resource Requirements

6.1 Certification body personnel

It is anticipated that, because of the GDPR articles specifying the elements of data protection certification, both legal and technical personnel will be required to be involved in assessment or evaluation and decision-making undertaken by certification bodies, in line with the certification scheme and depending on the Target of Evaluation or processing operation that is to be certified.

In addition to the requirements in section 6 of ISO 17065, the accreditation body shall ensure for each certification body that its personnel undertaking certification conformity tasks:

1. have demonstrated appropriate and ongoing expertise (knowledge and experience) with regard to data protection pursuant to Article 43 (1) of the GDPR, and related to the subject matter of the certification;
2. have independence and ongoing expertise with regard to the subject matter of certification pursuant to Article 43 (2) (a) of the GDPR and do not have a conflict of interest pursuant to Article 43 (2) (e) of the GDPR;
3. undertakes to respect the criteria referred to in Article 42 (5) pursuant to Article 43 (2) (b) of the GDPR;
4. have relevant and appropriate knowledge about and experience in applying data protection legislation;
5. have demonstrable, relevant and appropriate knowledge in applying data protection legislation in the context of the subject matter of the certification; and
6. are able to demonstrate experience in the fields mentioned in these additional requirements, specifically:

   <u>For personnel with technical expertise</u>:

   - Have obtained a qualification in a relevant area of technical expertise to at least EQF[4] level 6 or a recognised protected title (e.g. Dipl. Ing.) in the relevant regulated profession or have significant professional experience.
   - *Personnel responsible for certification decisions* require significant professional experience in data protection law, including identifying and implementing data protection measures, or access to someone with that expertise, and an appropriate professional/degree level qualification.
   - *Personnel responsible for evaluations* require relevant and recent professional experience and knowledge in technical data protection and experience in comparable procedures (e.g. certifications/audits), and appropriate professional qualifications where relevant.

   Personnel shall demonstrate that they maintain domain specific knowledge in technical and audit skills through continuous professional development.

   <u>For personnel with legal expertise</u>:

   - Legal studies at an EU or state-recognised university for at least eight semesters including the academic degree Master (LL.M.) or equivalent.
   - *Personnel responsible for certification decisions* shall demonstrate significant professional experience in data protection law, including identifying and implementing data protection

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

measures, or access to someone with that expertise, and an appropriate professional/degree level qualification.

- *Personnel responsible for evaluations* must demonstrate at least two years of professional experience in data protection law and knowledge and experience in technical data protection and comparable procedures (e.g. certifications/audits), and appropriate professional qualifications where relevant.

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

The certification body must be able to define and explain to the accreditation body which professional experience requirements are appropriate to the scope of the certification scheme and the ToE in question.

With respect to the requirements regarding personnel responsible for certification decisions, the certification body will retain the responsibility for the decision-making, even if it uses external experts. External actors shall not be involved in the decision making process.

If evaluation activities are outsourced to external bodies, those bodies shall be subject to the same conditions as the certification body. In particular, these data protection specific requirements have to be observed by the subcontracted body.

6.2 Resources for evaluation

The requirements in section 6.2 of ISO 17065 shall apply.

7 Process Requirements

7.1 General

In addition to the requirements in section 7.1 of ISO 17065, the accreditation body shall ensure the following:

1. Certification bodies comply with the additional requirements of the Norwegian SA (pursuant to Article 43 (1) (b) of the GDPR) when submitting the application in order that tasks and obligations do not lead to a conflict of interests pursuant to Article 43 (2) (e) of the GDPR;
2. The Norwegian SA and other relevant CSAs are notified before a certification body starts operating an approved European Data Protection Seal from an establishment or office in a new EEA Member State[5];
3. Certification bodies have procedures in place to notify the Norwegian SA immediately prior to issuing, renewing, withdrawing or rejecting certifications and provide the reasons for taking such actions. This includes providing to the Norwegian SA a copy of the executive summary of the evaluation report referenced in section 7.8 of this document; and
4. In cases where the client or the Norwegian SA notifies the certification bodies of any significant and relevant investigation or regulatory action by the Norwegian SA or other supervisory authorities within other sectors, that brings into question the client's data protection compliance, the certification bodies are required to make an assessment on whether the client still conforms with the certification criteria. The certification bodies will provide the Norwegian SA with a report advising of the outcome of this assessment. The assessment will be related to the scope of the certification and the ToE.

7.2 Application

In addition to the requirements in section 7.2 of ISO 17065, the certification body shall require that the application:

1. contains a detailed description of the ToE. This also includes interfaces and transfers to other systems and organisations, protocols and other assurances;
2. specifies whether processors are used, and when processors are the applicants, their responsibilities and tasks shall be described, and the application shall contain the relevant controller/processor contract(s);
3. specifies whether joint controllers are involved in the processing, and where the joint controller is the applicant, their responsibilities and tasks shall be described, and the application shall contain the agreement;
4. discloses any current or recent investigations or regulatory actions by the Norwegian SA or supervisory authorities within other sectors, to which the applicant is subject, if these investigations or regulatory actions concern processing of personal data related to the scope of certification and the ToE; and
5. in cases of data transfers to a third country or an international organisation, shall include a specification of the transferred data, the recipients of the data and a specification of the recipient's country and a specification of the provided data protection safeguards.

5 In this regard, see paragraph 44 of the EDPB Certification Guidelines.

7.3 Application review

In addition to the requirements in section 7.3 of ISO 17065, the accreditation body shall require that:

1. binding evaluation methods with respect to the ToE are laid down in the certification agreement;
2. the assessment in 7.3.1 (e) of whether there is sufficient expertise takes into account both technical and legal expertise in data protection to an appropriate extent; and
3. the application review shall take into account the data protection compliance checks referred to in 7.2 of this document. The certification body will be required to ensure that the applicant is a fit candidate for data protection certification.

7.4 Evaluation

In addition to the requirements in section 7.4 of ISO 17065, certification mechanisms shall describe sufficient evaluation methods for assessing the compliance of the processing operation(s) with the certification criteria, including such areas as:

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 evaluating 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 of the GDPR, and with regard to the definition of technical and organisational measures pursuant to Articles 24, 25 and 32 of the GDPR, insofar as the aforementioned Articles apply to the object of certification;
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 as set out in the criteria are met; and
4. documentation of methods and findings.

The certification body shall be required to ensure that these evaluation methods are standardised and applied consistently. This means that comparable evaluation methods are used for comparable ToEs. Any deviation from this procedure shall be justified by the certification body.

In addition to the requirements in section 7.4.2 of ISO 17065, the evaluation may be carried out by sub-contractors who have been recognised by the certification body, applying the same personnel requirements in section 6. If the evaluation is carried out by a sub-contractor, the sub-contractor must comply with the respective requirements of ISO 17065 and the additional requirements of the Norwegian SA. The use of sub-contractors does not exempt the certification body from its responsibilities.

In addition to the requirements in section 7.4.5 of ISO 17065, it shall be provided that existing certification in accordance with Articles 42 and 43 of the GDPR, which relates to the same ToE, may be taken into account as part of a new evaluation. However, the certificate alone will not be sufficient evidence, and the certification body shall be obliged to check the compliance with the criteria in respect of the ToE. The complete evaluation report and other relevant information enabling an evaluation of the existing certification and its results shall be considered in order to make an informed decision.

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.

In addition to the requirements in section 7.4.6 of ISO 17065, it shall be required that the certification body shall set out in detail in its certification scheme how the information required in section 7.4.6 of ISO 17065 informs the certification applicant about non-conformities with the scheme. In this context, at least the nature and timing of such information shall be defined. This is only applicable to certification bodies that are also scheme owners. The certification body shall set this out in a written document which could be either the certification scheme or, if the certification body is not the scheme owner, another document pertaining to the certification process.

In addition to the requirements in section 7.4.9 of ISO 17065, it shall be required that evaluation documentation be made fully accessible to the Norwegian SA upon request.

7.5 Review

In addition to the requirements in section 7.5 of ISO 17065, procedures for the granting, regular review and revocation of the respective certifications pursuant to Article 43 (2) and 43 (3) of the GDPR are required.

7.6 Certification decision

In addition to the requirements in section 7.6.1 of ISO 17065, the certification body shall be required to set out in detail in its procedures how its independence and responsibility with regard to individual certification decisions are ensured.

In addition to the requirements in section 7.6.2 of ISO 17065, immediately prior to issuing or renewing certification, the certification body shall be required to submit the draft approval, including the executive summary of the evaluation report to the Norwegian SA. The executive summary will clearly describe how the criteria are met thus providing the reasons for granting or maintaining the certification. The intention of this requirement is to increase transparency and the requirement does not entail a supervision of the draft approval.

In addition to the check carried out at the application stage, prior to issuing certification, the certification body shall be required to confirm with the applicant that they are not the subject of any Norwegian SA investigation or regulatory action in relation to the Target of Evaluation, which might prevent certification being issued. The Norwegian SA may confirm where appropriate that this is the case prior to the certification body issuing or renewing certification. If it is discovered that the applicant has not disclosed such action to the certification body, this may result in the certification not being issued.

In addition to the requirements in section 7.6.6 of ISO 17065, the certification body shall state where, how and when the applicant can appeal against the certification body’s decision not to grant certification, or apply for a review of that decision.

7.7 Certification documentation

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

In addition to the requirements in section 7.7.1 (e) of ISO 17065, it shall be required that the period of the intended monitoring within the meaning of section 7.9 will also be documented.

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

On issuing the certificate, the certification body shall be required to provide the Norwegian SA with a copy of the certification documentation referred to in 7.7.1 of ISO 17065.

7.8 Directory of certified products

In addition to the requirements in section 7.8 of ISO 17065, the certification body shall be required to keep the information on certified products, processes and services available internally and publicly.

The certification body will provide to the public an executive summary of the evaluation report. The aim of this executive summary is to help with transparency around what has been certified and how it was assessed. It will explain such things as:

a. the scope of the certification and a meaningful description of the ToE;
b. the respective certification criteria (including version or functional status);
c. the evaluation methods and tests conducted;
d. the result(s);
e. the date of granting and the date of expiration of the current certification; and
f. the initial and all re-certification dates.

In addition to the requirements in section 7.8 of ISO 17065 and pursuant to Article 43 (5) of the GDPR, the certification body shall inform in writing the Norwegian SA of the reasons for granting or revoking the requested certification.

7.9 Surveillance

In addition to the requirements in sections 7.9.1, 7.9.2 and 7.9.3 of ISO 17065, and according to Article 43 (2) (c) of the GDPR, it shall be required that regular monitoring measures are obligatory to maintain certification during the monitoring period. Such measures shall be risk based and proportionate and the maximum period between surveillance activities shall not exceed 12 months.

7.10 Changes affecting certification

In addition to the requirements in sections 7.10.1 and 7.10.2 of ISO 17065, changes affecting certification to be considered by the certification body shall include:

- any personal data breach, or infringement of GDPR or the PDA18 established by the Norwegian SA, supervisory authorities within other sectors and/or judicial authorities, that relates to the certification, reported by the client or the Norwegian SA;
- changes in the state of art technology (as far as relevant for the future certification and surveillance);
- amendments to data protection legislation;
- the adoption of delegated acts of the European Commission in accordance with Articles 43 (8) and 43 (9) of the GDPR;
- decisions, opinions, guidelines, recommendations, best practices or other documents adopted by the EDPB; and
- court decisions related to data protection.

The change procedures to be implemented by the certification body shall include such things as: transition periods, approvals process with the Norwegian SA, reassessment of the relevant ToE, and appropriate measures to revoke the certification if the certified processing operation is no longer in compliance with the updated criteria.

7.11 Termination, reduction, suspension or withdrawal of certification

In addition to the requirements in section 7.11.1 of ISO 17065, and section 7.1 (3) of this document, the certification body shall be required to inform the Norwegian SA and the accreditation body where relevant immediately in writing about measures taken and about continuation, restrictions, suspension and withdrawal of certification.

Furthermore, in cases where the certification body determines non-compliance, it must define in its requirements what measures are to be taken.

According to Article 58 (2) (h) of the GDPR, the certification body shall be required to accept decisions and orders from the Norwegian SA to withdraw or not to issue certification to a client (applicant) if the requirement for certification are not or no longer met. In such cases, the certification body shall provide clear and documented evidence to the Norwegian SA that proper action has been taken.

7.12 Records

In addition to the requirements of ISO 17065, the certification body is required to keep all documentation complete, comprehensible, up-to-date and fit for audit.

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

In addition to the requirements in section 7.13.1 of ISO 17065, the certification body shall 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.

In addition to the requirements in section 7.13.2 of ISO 17065, the certification body shall be required to define:

a. how and to whom such confirmation must be given;
b. the deadlines for this; and
c. which processes are to be initiated afterwards.

In addition to the requirements in sections 7.13.7 and 7.13.8 of ISO 17065, the certification body shall be required to define reasonable time limits for properly informing the complainants about the progress, the outcome and the end of the complaint process.

Certification bodies shall be required to make their complaints handling procedures publicly available and easily accessible to data subjects.

The certification body shall be required to inform complainants of the progress and the outcome of the complaint within a reasonable period.

In addition to the requirements in section 7.13.1 of ISO 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 section 8 of ISO 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 with the accredited body itself.

In addition to the requirements in section 8 of ISO 17065, management principles and their documented implementation must be transparent and be disclosed by the accredited certification body at the request of the Norwegian SA at any time during an investigation in the form of data protection audits pursuant to Article 58 (1) (b) of the GDPR or a review of the certifications issued in accordance with Article 42 (7) pursuant to Article 58 (1) (c) of the GDPR.

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) as well as how long the certifications are valid under which framework and conditions (recital 100 of the GDPR).

The procedures in the event of suspension or withdrawal of the accreditation shall be integrated into the management system of the certification body, including notification to their clients.

A complaints handling process with the necessary levels of independence shall be established by the certification body as an integral part of the management system, which shall in particular implement the requirements of sections 4.1.2.2 (c), 4.1.2.2 (j), 4.6 (d) and 7.13 of ISO 17065. Relevant complaint and objections shall be shared with the Norwegian SA.

8.1 General management system requirements

The requirements in section 8.1 of ISO 17065 shall apply.

8.2 Management system documentation

The requirements in section 8.2 of ISO 17065 shall apply.

8.3 Control of documents

The requirements in section 8.3 of ISO 17065 shall apply.

8.4 Control of records

The requirements in section 8.4 of ISO 17065 shall apply.

8.5 Management Review

The requirements in section 8.5 of ISO 17065 shall apply.

8.6 Internal audits

The requirements in section 8.6 of ISO 17065 shall apply.

8.7 Corrective actions

The requirements in section 8.7 of ISO 17065 shall apply.

8.8 Preventive actions

The requirements in section 8.8 of ISO 17065 shall apply.

9 Further Additional Requirements

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 section 7.4 of ISO 17065 and this document. 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 section 9.1 of this document.

9.3 Responsibilities and competences

9.3.1 Communication between CB and its clients and applicants

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

1. Maintaining documentation of tasks and responsibilities by the accredited certification body, for the purposes of:
    a. responding to information requests; or
    b. to enable contact in the event of a complaint about a certification.
2. Maintaining an application process for the purposes of:
    a. Information on the status of an application; and
    b. Evaluations by the Norwegian SA with respect to:
        i. Feedback; and/or
        ii. Decisions by the Norwegian SA.

9.3.2 Documentation of evaluation activities

Systems shall be in place for implementing appropriate procedures and communication structures between the certification body and the Norwegian SA.

This shall include a reporting framework to inform the Norwegian SA:

- of details of applicant on receipt of application to enable the Norwegian SA to check its records for the applicant's compliance history as per section 7.6 of this document; and
- of the reasons for granting/withdrawing/rejecting certification pursuant to Article 43 (5) of the GDPR, immediately prior to issuing, renewing, suspending or withdrawing certifications as per section 7.1 (3) of this document.

9.3.3 Management of complaint handling

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

Relevant complaints and objections shall be shared with the Norwegian SA upon request.

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 the notification of clients.

Address:
Trelastgata 3, Oslo, Norway

P.O. Box:
Postboks 458 Sentrum,
0105 Oslo
Norway

postkasse@datatilsynet.no
Phone: +47 22 39 69 00

datatilsynet.no
personvernbloggen.no