Danish accreditation requirements for certification bodies

March 2021

DATATILSYNET

Content

Prefix

According to Paragraph 25 of the Danish Data Protection Act[1] the Danish Data Protection Agency (Danish DPA) and the Danish Accreditation Fund (DANAK) both are empowered to grant accreditation to certification bodies in accordance with Article 43(1) (a) and (b) of the General Data Protection Regulation (GDPR).

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

The terms of cooperation between the Danish DPA and DANAK as the Danish National Accreditation Body (NAB) are set out in an accreditation message drafted by DANAK and the Danish DPA. The accreditation message sets out the roles, responsibilities and operational procedures in relation to accreditation for GDPR certification schemes. The accreditation message is available at both the Danish DPA's and DANAK's website.

If at some point the Danish DPA chooses to use its empowerment to grant accreditation in accordance with Paragraph 25 of the Danish Data Protection Act, the Danish DPA 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 Danish DPA where the additional requirements now refers to the accreditation body.

1 The Danish Data Protection Act 2018 (Act No. 502 of 23 May 2018 as amended)

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[2] and certification[3] 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 controller and processor's processing operations.

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

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

2. Normative reference

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 guidelines on accreditation and certification shall apply and have precedence over ISO definitions. For ease of reference, the main definitions used in this document are listed below.

General Data Protection Regulation (GDPR): Regulation 2016/679/EC

DPA18: The Danish Data Protection Act 2018 (Act No. 502 of 23 May 2018 as amended)

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

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

ISO 17065: ISO/IEC 17065/2012

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

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 guidelines on accreditation.

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 Denmark, the NAB is the Danish Accreditation Fund (DANAK).

Accreditation body: Body that performs accreditation. In this document, this term is taken to mean DANAK. If at some point, the Danish DPA chooses to use its empowerment to grant accreditation in accordance with Paragraph 25 of the DPA18, the term is taken to mean the Danish DPA.

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 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.

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.

Competent supervisory authority: Where referred to in this document means the Danish Data Protection Agency.

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

Applicant: The organisation that has applied to have their processing operations certified.

Client[4]**:** The organisation that has been certified (previously the applicant).

[4] 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

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 DPA18. 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 – and have not previously been – the subject of any investigation or regulatory action by the Danish DPA, which may mean they do not meet this requirement and therefore might prevent their accreditation. Before proceeding with the accreditation process, the accreditation body will contact the Danish DPA in order to verify this information. The Danish DPA will verify the information where appropriate. .

The certification body shall also confirm to the accreditation body that they are not – and have not previously been – the subject of any investigation or 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 this requirement, and therefore might prevent their accreditation.

The certification body shall inform the accreditation body immediately of relevant infringements of GDPR or the DPA18 established by the Danish DPA, 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 inform the Danish DPA pursuant to Article 43 (1) of the GDPR.

The Danish DPA 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 ISO 17065 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 (a) ISO 17065 and the criteria approved by the Danish DPA 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 Danish DPA 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 is 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 4.1.2.2 (c) (1) 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 Danish DPA all information necessary for granting the certification pursuant to Articles 42 (8) and 43 (5) of the GDPR respectively,

8. include rules on the necessary precautions for the investigation of complaints within the meaning of 4.1.2.2 (c)(2), additionally, (j) ISO 17065, 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 4.1.2.2 ISO 17065, if the consequences of withdrawal or suspension of accreditation for the certification body impact on the client, in that case the consequences for the customer should also be addressed,

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.

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 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 17065

1. the certification body comply with the additional requirements of the Danish DPA (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,

    b. 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 customer it assesses, including for example:
    a. Any type of economic relation between the certification body and the customer, 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 customer it assesses.
    c. The certification body may not be controlled in any way by the customer it assesses.
    d. The certification body may not be in a controller/processor relationship with the customer it assesses.

4.3 Liability and financing

The accreditation body shall in addition to the requirement in 4.3.1 ISO 17065 ensure on a regular 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

Requirements of ISO 17065 shall apply.

4.5 Confidentiality

Requirements of ISO 17065 shall apply.

4.6 Publicly available information

In addition to the requirement in 4.6 ISO 17065, the accreditation body shall 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;

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

5. Structural requirements - and Article 43 (4) of the GDPR (“proper assessment”)

5.1 Organisational structure and top management

Requirements of ISO 17065 shall apply

5.2 Mechanisms for safeguarding impartiality

Requirements of ISO 17065 shall apply.

6. Resource requirements

6.1 Certification body personnel

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

1. has demonstrated appropriate and ongoing expertise (knowledge and experience) with regard to data protection pursuant to Article 43 (1) of the GDPR,

2. has independence and ongoing expertise with regard to the object 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. 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 these additional requirements, specifically:

   For personnel with technical expertise:

   - Have obtained a qualification in a relevant area of technical expertise to at least EQF[5] 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 they maintain 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 significant professional experience.

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

- *Personnel responsible for certification decisions* shall demonstrate 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* 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 should not be involved in the decision making process.

6.2 Resources for evaluation

Requirements of ISO 17065 shall apply.

7. Process requirements, Article 43 (2)(c), (d) of the GDPR

7.1 General

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

1. Certification bodies comply with the additional requirements of the Danish DPA (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 relevant competent supervisory authority is notified pursuant to Article 43 (1) of the GDPR, before other establishments or offices of the certification body starts operating an approved European Data Protection Seal in a new Member State.[6]

3. Certification bodies have procedures in place to notify the Danish DPA immediately prior to issuing, renewing or withdrawing certifications and provide the reasons for taking such actions. This includes providing the Danish DPA a copy of the executive summary of the evaluation report referenced in section 7.8 of this document.

4. In cases where the client or the Danish DPA notifies the certification bodies of any significant and relevant investigation or regulatory action by the Danish DPA 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 Danish DPA 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 item 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 applicant, 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 whether the joint controller is the applicant, their responsibilities and tasks shall be described, and the application shall contain the agreed agreement, and

4. discloses any current or recent investigations or regulatory actions by the Danish DPA 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.

The certification body shall be required to inform the Danish DPA in writing when it receives an application.

6 In this regard, see Guidelines 1/2018, paragraph 44.

7.3 Application review

In addition to item 7.3 of ISO 17065, the accreditation body shall require that:

1. binding evaluation methods with respect to the Target of Evaluation (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.

7.4 Evaluation

In addition to item 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, 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 as set out in the adopted criteria are met, and

4. documentation of methods and findings.

The certification body shall be required to ensure that these evaluation methods are standardized 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 item 7.4.2 of ISO 17065 the evaluation may be carried out by sub-contractors who have been recognised by the certification body, using 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 Danish DPA. The use of sub-contractors does not exempt the certification body from its responsibilities.

In addition to item 7.4.5 of ISO 17065, it shall be provided that existing certification, 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 item 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 item 7.4.6 informs the certification applicant about nonconformities with the scheme. In this context, at least the nature and timing of such information shall be defined. 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 item 7.4.9 of ISO 17065, it shall be required that evaluation documentation be made fully accessible to the Danish DPA upon request.

7.5 Review

In addition to item 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 point 7.6.1 of ISO 17065, the certification body should 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 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 Danish DPA. 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 investigation or regulatory action by the Danish DPA in relation to the ToE which might prevent certification being issued. The Danish DPA will confirm where appropriate that this is the case prior to the certification body issuing or renewing certification.

The certification body shall also be required to confirm with the applicant that they are not subject of any investigation or regulatory action by other supervisory authorities within other sectors, if these investigations or regulatory actions concern processing of personal data and might prevent certification being issued.

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.

7.7 Certification documentation

In addition to item 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 item 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 item 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 Danish DPA 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 item 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 available.

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 object of certification (ToE),

b) the respective certification criteria (including version or functional status),

c) the evaluation methods and tests conducted and

d) the result(s).

In addition to item 7.8 of ISO 17065 and pursuant to Article 43(5) of the GDPR, the certification body shall inform in writing the Danish DPA 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 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 should be risk based and proportionate and the maximum period between surveillance activities should not exceed 12 months.

7.10 Changes affecting certification

In addition to points 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 DPA18 established by the Danish DPA, supervisory authorities within other sectors and/or judicial authorities that relates to the certification, reported by the client or the Danish DPA
- 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 competent supervisory authority, 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 point 7.11.1 of ISO 17065, and section 7.1(3) of this document, the certification body shall be required to inform the Danish DPA and the accreditation body where relevant immediately in writing about measures taken and about continuation, restrictions, suspension and withdrawal of certification.

According to Article 58 (2)(h) of the GDPR, the certification body shall be required to accept decisions and orders from the Danish DPA 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

In addition to the requirements of ISO 17065, the certification body is 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 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 item 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 time limits for this; and

c) which processes are to be initiated afterwards.

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 item 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 chapter 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 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 Danish DPA 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.

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 and applicants.

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 points 4.1.2.2(c), 4.1.2.2(j), 4.6(d) and 7.13 of ISO 17065. Relevant complaint and objections should be shared with the competent supervisory authority.

8.1 General

Requirements of ISO 17065 shall apply.

8.2 Management system documentation

Requirements of ISO 17065 shall apply.

8.3 Control of documents

Requirements of ISO 17065 shall apply.

8.4 Control of records

Requirements of ISO 17065 shall apply.

8.5 Management review

Requirements of ISO 17065 shall apply.

8.6 Internal audits

Requirements of ISO 17065 shall apply.

8.7 Corrective actions

Requirements of ISO 17065 shall apply.

8.8 Preventive actions

Requirements 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 point 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 point 9.1 of this document.

9.3 Responsibilities and competencies

9.3.1 Communication between certification body and its clients and applicants

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) 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 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.

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 Danish DPA. This shall include a reporting framework to inform the Danish DPA:

- of details of applicant on receipt of application to enable the Danish DPA to check its records for the applicant's compliance history as per section 7.6 of this document;
- of the reasons for granting/withdrawing 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.

.

Danish accreditation requirements for certification bodies

Udgivet af:
Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 33 19 32 00
dt@datatilsynet.dk
datatilsynet.dk

Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 33 19 32 00
dt@datatilsynet.dk
datatilsynet.dk