Additional Accreditation Requirements for Certification Bodies

V. 0.3 – 28.07.2025

CONTENTS Page

Introduction 3

Prefix 3

1. Scope 3

2. Normative Reference 4

3. Terms and Definitions 4

4. General Requirements for Accreditation 5

4.1 Legal and contractual matters 5

4.1.1 Legal Responsibility 5

4.1.2 Certification agreement ("CA") 6

4.1.3 Use of data protection seals and marks 7

4.2 Management of Impartiality 8

4.3 Liability and financing 8

4.4 Non-discriminatory conditions 8

4.5 Confidentiality 9

4.6 Publicly available information 9

5. Structural Requirements 9

5.1 Organisational structure and top management 9

5.2 Mechanisms for safeguarding impartiality 9

6. Resource requirements 9

6.1 Certification body personnel 9

6.2 Resources for evaluation 11

7. Process Requirements (Article 43(2)(c),(d) GDPR) 11

7.1 General 11

7.2 Application 12

7.3 Application Review 12

7.4 Evaluation 13

7.5 Review 14

7.6 Certification decision 14

7.7 Certification documentation 15

7.8 Directory of certified products 15

7.9 Surveillance 16

7.10 Changes affecting certification 16

7.11 Termination, reduction, suspension or withdrawal of certification 17

7.12 Records 17

7.13 Complaints and appeals (Article 43(2)(d) GDPR) 17
8. Management and system requirements 18
8.1 General management system requirements 19
8.2 Management system documentation 19
8.3 Control of documents 19
8.4 Control of records 19
8.5 Management review 19
8.6 Internal audits 20
8.7 Corrective actions 20
8.8 Preventive actions 20
9. Further additional requirements 20
9.1 updating of evaluation methods 20
9.2 Maintaining expertise 20
9.3 Responsibilities and competencies 20
9.3.1 Communication between the certification body and its customers 20
9.3.2 Communication between the certification body, the Malta SA and the NAB 21
9.3.3 Documentation of evaluation activities 21
9.3.4 Management of complaint handling 21
9.3.5 Management of withdrawal 22

Introduction

This document establishes the Office of the Information and Data Protection Commissioner's (the "**Malta SA**") additional accreditation requirements complementing Regulation (EC) No 765/2008[1], and the technical rules describing the methods and procedures relating to certification bodies. This document is issued pursuant to Article 43(1)(b) and 43(3) of Regulation (EU) 2016/679[2] ("GDPR").

Prefix

Pursuant to Article 32(1) of the Data Protection Act (Cap. 586 of the Laws of Malta), certification bodies referred to in Article 43 GDPR are accredited by the National Accreditation Board (Malta)[3] (the "**NAB**") in accordance with ISO/IEC 17065/2012[4] ("**ISO 17065**") and with the additional accreditation requirements set herein.

The relationship between the Malta SA and the NAB is governed by a cooperation agreement, a summary of which is available on the Commissioner's website[5] [NOT YET AVAILABLE].

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 (the "**EDPB**") guidelines on accreditation[6] (hereinafter "guidelines on accreditation") and certification[7] (hereinafter "guidelines on certification") provide further information.

[1] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93.
[2] 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 (General Data Protection Regulation).
[3] The National Accreditation Board (Malta) is established by regulation 3 of the National Accreditation Board (Malta) (Establishment) Regulations (Subsidiary Legislation 419.07).
[4] ISO/IEC 17065:2012 Conformity assessment — Requirements for bodies certifying products, processes and services. See https://www.iso.org/standard/46568.html (last seen on 13th October 2022).
[5] Not yet available.
[6] EDPB, *Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)*, V. 3.0, 4 June 2019.
[7] EDPB, *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation*, V. 3.0, 4 June 2019.

The scope of a certification mechanism shall be taken into account in the assessment by the NAB during the accreditation process, particularly with respect to criteria, expertise and evaluation methodology.

The broad scope of ISO 17065 covering products, processes and services should not lower or override the requirements of the GDPR. Thus, it remains necessary that a certification mechanism relates to the processing of personal data. Pursuant to Article 42(1) GDPR, GDPR certification is only applicable to the processing operations of controllers and processors.

2. Normative Reference

The GDPR has precedence over ISO 17065. If the additional requirements or the certification mechanism make reference 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 guidelines on accreditation and guidelines on certification shall apply, and have precedence over ISO definitions. For ease of reference the main definitions used in this document are listed below.

The following terms shall have the same meaning as in article 4 GDPR: “personal data”, “processing”, “controller”, “processor”, “personal data breach” and “supervisory authority”. The term “joint controllers” shall have the same meaning as in article 26(1) GDPR.

“accreditation”	An attestation by the National Accreditation Board that a certification body is qualified to carry out certification pursuant to Article 42 and 43 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 GDPR, see section 3 of the guidelines on accreditation.
“applicant”	The organisation that has applied to have its processing operations certified.
“certification”	The assessment and impartial, third-party attestation that the fulfilment of certification criteria has been demonstrated in respect of one or more controller or processor’s processing operations.
“certification body”	Third party conformity assessment body operating certification scheme.
“certification criteria”	The criteria against which an applicant’s processing operations are measured for a given certification scheme.
“certification	An approved certification scheme which is available to the applicant. It is a service

mechanism"	provided by a certification body based on approved criteria and assessment methodology. It is the system by which data processing operations of a controller or processor becomes certified.
"certification scheme"	A certification system related to data processing operations to which the same specified requirements, specific rules and procedures apply. It includes the certification criteria and assessment methodology.
"client"	The organisation that has been certified (previously the applicant). Whenever the term "client" is used in the International Standard (ISO/IEC 17065), it applies to both the "applicant" and the "client", unless otherwise specified.
"National Data Protection Legislation"	Data Protection Act (Cap. 586 of the Laws of Malta) and subsidiary legislation issued thereunder.
"target of evaluation"	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.

4. General Requirements for Accreditation

4.1 Legal and contractual matters

4.1.1 Legal Responsibility

In both cases of first-time accreditation and renewal of previously granted accreditation, a certification body shall be able to demonstrate (at all times) to the NAB 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 same goes for the certification body's capability to demonstrate that its procedures and measures specifically for controlling and handling of applicants' or clients' personal data as part of the certification process, are compliant with GDPR and with National Data Protection Legislation.

As such, it shall provide evidence of compliance as required during both the first-time accreditation process and the process of renewal of the accreditation, as the case may be.

This shall include the certification body confirming to the NAB that they are not subject to any investigation or regulatory action by the Malta SA in relation to the target of evaluation, which may mean they do not meet this requirement and therefore might prevent their accreditation. Before proceeding with the accreditation process, the NAB shall contact the Malta SA in order to verify this information. In case any such investigation or regulatory action by the Malta SA on the certification body is ongoing or has been

concluded, the NAB and the Malta SA shall exchange all the information required between them pursuant to the provisions of the cooperation agreement concluded between them.

The certification body shall inform the NAB immediately about infringements of GDPR or of National Data Protection Legislation established by the MT SA and / or judicial authorities in relation to the target of evaluation which may affect its accreditation.

Prior to issuing or renewing a certification, the certification body shall be required to inform the Malta SA pursuant to Article 43(1) GDPR and as further prescribed in sub-section 7.6 of this document.

4.1.2 Certification agreement ("CA")

The certification body shall demonstrate that its certification agreements fulfill the following requirements in addition to the requirements of clause 4.1.2.1 of ISO 17065:

a. require the applicant to always comply with both the general certification requirements within the meaning of sub-clause 4(1)(2)(2)(a) of ISO 17065 and with the criteria approved by the Malta SA in accordance with Article 43(2)(b) GDPR, or by the EDPB in accordance with Article 42(5) GDPR;

b. require the applicant to allow full transparency to the Malta SA with respect to the certification procedure, including contractually confidential materials whether contractual or otherwise, related to data protection compliance pursuant to Articles 42(7) and 58(1)(c) GDPR;

c. do not reduce the responsibility of the applicant for compliance with GDPR and is without prejudice to the tasks and powers of the Malta SA in line with Article 42(5) GDPR;

d. 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) GDPR;

e. 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;

f. with respect to sub-clause 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) GDPR including rules setting appropriate intervals for re-evaluation or review (regularity) in line with Article 42(7) GDPR and with section 7(9) of this document;

g. require the applicant to allow the certification body to disclose to the Malta SA all information necessary for granting the certification pursuant to Articles 42(8) and 43(5) GDPR;

h. include rules on the necessary precautions for the investigation of complaints within the meaning of sub-clause 4(1)(2)(2)(c)(2) of ISO 17065. Additionally, lit. j shall also contain explicit statements on the structure and the procedure for complaint management in accordance with Article 43(2)(d) GDPR;

i. require in addition to the minimum requirements referred to in ISO 17065 sub-clause 4(1)(2)(2), if the consequences of withdrawal or suspension of accreditation for the certification body impact on the client, that the consequences for the customer are addressed, for example by making all necessary modifications to formal certification documents, public information, authorizations for use of marks, etc., in order to ensure it provides no indication that products, processes and services continues to be certified

j. require the applicant to inform the certification body in the event of significant changes in its factual or legal situation and in its products, processes and services, concerned by the certification. In this respect, the application shall inform the certification body of any infringements of the GDPR established by the MT SA and/or judicial authorities that may affect certification and

k. includes binding evaluation methods with respect to the target of evaluation.

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 GDPR and with the guidelines on accreditation and certification.

4.2 Management of Impartiality

The NAB shall ensure that in addition to the requirements of clause 4(2) of ISO 17065, the certification body:

a. complies with the additional requirements established herein by the Malta SA pursuant to Article 43(1)(b) GDPR;

b. in line with Article 43(2)(a) GDPR, provides 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;

c. has demonstrated that its tasks and obligations do not lead to a conflict of interest pursuant to Article 43(2)(e) GDPR; and

d. has established clear rules to prevent conflicts of interest and in case conflicts of interest are identified, to manage them; and

e. has no relevant connection with the applicant it assesses.

By way of example, the following scenarios may affect the impartiality of the certification body's activities:

a. the certification body forming part of the same company, group and, or legal entity as the client undergoing scrutiny; and, or

b. the certification body being controlled by the client undergoing scrutiny, by virtue, for example, of ownership, financial participation or the rules which govern it.

4.3 Liability and financing

The NAB shall, in addition to the requirements of clause 4(3)(1) of 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

The Requirements of clause 4(4) of ISO 17065 shall apply.

4.5 Confidentiality

The requirements of clause 4(5) of ISO 17065 shall apply.

4.6 Publicly available information

In addition to the requirements of clause 4(6) of ISO 17065, the NAB shall require from the certification body that, as a minimum:

a. all versions (current and previous) of the approved criteria used within the meaning of Article 42(5) GDPR are published and easily publicly available as well as all certification procedures, generally stating the respective period of validity; and

b. information about complaints handling procedures and appeals is made public pursuant to Article 43(2)(d) GDPR.

5. Structural Requirements

5.1 Organisational structure and top management

The requirements of clause 5(1) of ISO 17065 shall apply.

5.2 Mechanisms for safeguarding impartiality

The requirements of clause 5(2) of ISO 17065 shall apply.

6. Resource requirements

6.1 Certification body personnel

In addition to the requirements in clause 6 of ISO 17065, the NAB shall ensure for each certification body that its personnel:

a. has demonstrated appropriate and ongoing expertise (knowledge and experience) regarding data protection pursuant to Article 43(1) GDPR;

b. has independence and ongoing expertise with regard to the target of evaluation pursuant to Article 43(2)(a) GDPR, and does not have a conflict of interest pursuant to Article 43(2)(e) GDPR;

c. undertakes to respect the criteria referred to in Article 42(5) pursuant to Article 43(2)(b) GDPR;

d. has relevant and appropriate knowledge about and experience in applying data protection legislation;

e. has relevant and appropriate knowledge about and experience in technical and organisational data protection measures as relevant; and

f. is able to demonstrate experience in the fields mentioned in the additional requirements of clauses 6(1)(1), 6(1)(4) and 6(1)(5) of ISO 17065, specifically:

For personnel with technical expertise:

- having obtained a qualification in a relevant area of technical expertise to at least EQF[8] 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* shall demonstrate at least two years professional experience in technical data protection , including in identifying and implementing data protection measures;

- *personnel responsible for evaluations* require shall demonstrate at least two years of relevant professional experience in technical data protection, and knowledge of and experience in comparable procedures (e.g., certifications/audits). Where relevant, experience shall be demonstrated by means of appropriate professional qualifications; and

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

For personnel with legal expertise:

- legal studies pursued at an EU or state-recognised university for at least eight semesters awarded with an academic degree Master (LL.M.) or equivalent;

[8] See European Qualifications Framework. See qualification framework comparison tool on: https://europa.eu/europass/en/compare-qualifications (last seen on 13th October 2022).

- *personnel responsible for certification decisions* shall demonstrate significant professional experience in data protection law, including identifying and implementing data protection measures;

- *personnel responsible for evaluations* must demonstrate at least two years of professional experience in data protection law and knowledge and experience in comparable procedures (e.g., certifications/audits); and

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

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 must be observed by the subcontracted body.

6.2 Resources for evaluation

The requirements of clause 6(2) of ISO 17065 shall apply.

7. Process Requirements (Article 43(2)(c),(d) GDPR)

7.1 General

In addition to the requirements of section 7(1) of ISO 17065, the NAB shall be required to ensure that:

a. certification bodies comply with the additional requirements of the Malta SA (pursuant to Article 43(1)(b) 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);

b. all relevant the relevant supervisory authorities are notified before a certification body starts operating an approved European Data Protection Seal[9] in a new Member State from a satellite office;

[9] See Article 42(5) GDPR.

c. certification bodies have procedures in place to notify the Malta SA immediately prior to issuing, renewing, withdrawing certifications and provide the reasons for taking such actions. This shall include providing the Malta SA with a copy of the executive summary of the evaluation report referenced in section 7(8) of this document; and

d. the certification body have established procedures to investigate where the client or the Malta SA notifies it of any significant and relevant investigation or regulatory action by the Malta SA in relation to the scope of the certification and the target of evaluation that brings into question the client's data protection compliance. In such instances, the certification body will undertake an investigation to the extent appropriate and make an assessment as to whether the client still conforms to the certification criteria. The certification body shall provide the Malta SA with a report outlining the outcome of said assessment.

7.2 Application

In addition to clause 7(2) of ISO 17065, the certification body shall require from the applicant to:

a. includes a detail description of the object of the certification, being the target of evaluation. This also includes interfaces and transfers to other systems and organisations, protocols and other assurances;

b. specifiy whether processors are used. When the processors are the applicants, their responsibilities and tasks shall be described, and the application shall contain the relevant controller / processor contract(s). Likewise, the certification body shall require the applicant to specify whether it acts as a joint controller. Should that be the case, the certification body shall provide a copy of the arrangement concluded between the joint controllers; and

c. disclose any current or recent investigations or regulatory actions related to the scope of certification and target of evaluation, of the Malta SA to which the applicant is or has been subject.

The certification body shall inform the Malta SA when it receives an application.

7.3 Application Review

In addition to clause 7(3) of ISO 17065, it is required that:

a. binding evaluation methods with respect to the target of evaluation are laid down in the certification agreement;

b. the assessment in sub-clause 7(3)(1)(e) of ISO 17065 as to whether there is sufficient expertise takes into account both technical and legal expertise in data protection is executed to an appropriate extent; and

c. application review takes into account the data protection compliance checks referred to in section 7(2)(3) of this document. The certification body will be required to ensure that the application is a fit candidate for data protection certification.

7.4 Evaluation

In addition to the requirements of clause 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 for example where applicable:

a. a method for assessing the necessity and proportionality of processing operations in relation to their purpose and the rights of data subjects concerned;

b. 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, 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 articles apply to the target of evaluation;

c. 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 target of evaluation and to demonstrate that the legal requirements as set out in the adopted criteria are met; and

d. 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 targets of evaluation. Any deviation from this procedure shall be justified by the certification body.

In addition to clause 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 as those contained in section 6(1) of this document. The use of sub-contractors does not exempt the certification body from its responsibilities.

In addition to clause 7(4)(5) of ISO 17065, it shall be provided that existing certification, which relates to the same target of evaluation, may be taken into account as part of a new evaluation. However, existing data protection certification alone will not be sufficient evidence to completely replace (partial) evaluations, and the certification body shall be obliged to check the compliance with the criteria in respect of the target of the evaluation. 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 accordance with Article 42 and 43 GDPR, a certification statement or similar certification certificates should not be considered sufficient to replace a report.

In addition to clause 7(4)(6) of ISO 17065, it shall be required that the certification body sets out in detail in its certification scheme how the information required in clause 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.

In addition to clause 7(4)(9) of ISO 17065, it shall be required that evaluation documentation be made fully accessible to the Malta SA upon request.

7.5 Review

In addition to clause 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) GDPR are required.

7.6 Certification decision

In addition to clause 7(6)(1) of ISO 17065, the certification body shall be required to set out in detail in its procedures how its independence and responsibilities 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 Malta SA. The executive summary will clearly describe how the criteria are met thus providing the reasons for granting or maintaining the certification. The purpose of this requirement is to increase transparency, and it does not entail a supervision of the draft approval.

In addition to the checks carried out at application stage, prior to issuing or renewing the 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 Malta SA, by any other supervisory authority within and, or by competent judicial authorities in relation to the target of evaluation which might prevent certification being issued. The Malta SA will 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 any such action to the certification body, this may result in the certification not being issued.

7.7 Certification documentation

In addition to sub-clause 7(7)(1)(e) of ISO 17065 and in accordance with Article 42(7) GDPR, it shall be required that the period of validity of certifications shall not exceed three years.

In addition to sub-clause 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) herein will also be documented.

In addition to sub-clause 7(7)(1)(f) of ISO 17065, the certification body shall be required to name the target of evaluation 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 Malta SA with a copy of the certification documentation referred to in clause 7(7)(1) of ISO 17065.

7.8 Directory of certified products

In addition to the requirements of clause 7(8) of ISO 17065, the certification body shall be required to keep the information on certified products, processes and services available internally and to make publicly available a record of the certifications issued, including information about the certification mechanism and how long the certifications are valid for.

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 target of evaluation;

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

c. the evaluation methods and tests conducted; and, or

d. the result(s).

In addition to clause 7(8) of ISO 17065 ad pursuant to Article 43(5) GDPR, the certification body shall proactively inform the Malta SA of the reasons for granting or revoking the requested certification.

7.9 Surveillance

In addition to clauses 7(9)(1), 7(9)(2) and 7(9)(3) of ISO 17065, and according to Article 43(2)(c) 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 twelve (12) months.

7.10 Changes affecting certification

In addition to clauses 7(10)(1) and 7(10)(2) of ISO 17065, changes affecting certification to be considered by the certification body shall include:

a. amendments to data protection legislation;

b. the adoption of delegated acts by the European Commission in accordance with Articles 43(8) and 43(9) GDPR;

c. issuance of decisions by the EDPB;

d. issuance of court decisions related to data protection;

e. any personal data breach, or any infringement of GDPR and, or National Data Protection Legislation established by the Malta SA or by competent judicial authorities in relation to the subject matter of certification, reported either by the client or by the Malta SA; and, or

f. changes in the state-of-the-art technology, insofar as relevant in relation to the target of evaluation.

The change in procedures to be implemented by the certification body shall include such things as: transition periods, approvals process with the Malta SA, reassessment of the relevant target of evaluation 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 clause 7(11)(1) of ISO 17065 and to section 7(1)(c) of this document, the certification body shall be required to immediately inform in writing the Malta SA (and the NAB, where relevant) about the measures taken and about the continuation, restrictions, suspension and withdrawal of certification.

According to Article 58(2)(h) GDPR, the certification body shall be required to accept decisions and orders from the Malta SA to withdraw or not to issue certification to a client if the requirements 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) GDPR)

In addition to clause 7(13)(1) of ISO 17065, the certification body shall 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 clause 7(13)(2) of ISO 17065, the certification body shall 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 sure that their complaints handling procedures are publicly available and easily accessible to data subjects.

In addition to the requirements of clauses 7(13)(7) and 7(13)(8) of ISO 17065, the certification body shall be required to define reasonable time limits for properly informing complainants of the progress and the outcome of their complaints.

In addition to clauses 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 and 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 Belgian DPA at any time during an investigation in the form of data protection audits pursuant to Article 58(1)(b) GDPR or a review of the certifications issued in accordance with Article 42(7) pursuant to Article 58(1)(c) 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 frameworks 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 and applicants.

A complaint-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 sub-clauses 4(1)(2)(2)(c), 4(1)(2)(2)(j), 4(6)(d) and clause 7(13) of ISO 17065.

8.1 General management system requirements

The requirements of clause 8(1) of ISO 17065 shall apply.

8.2 Management system documentation

The requirements of clause 8(2) of ISO 17065 shall apply.

8.3 Control of documents

The requirements of clause 8(3) of ISO 17065 shall apply.

8.4 Control of records

The requirements of clause 8(4) of ISO 17065 shall apply.

8.5 Management review

The requirements of clause 8(5) of ISO 17065 shall apply.

8.6 Internal audits

The requirements of clause 8(6) of ISO 17065 shall apply.

8.7 Corrective actions

The requirements of clause 8(7) of ISO 17065 shall apply.

8.8 Preventive actions

The requirements of clause 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 clause 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 competencies

9.3.1 Communication between the certification body and its customers

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

a. maintaining documentation of tasks and responsibilities by the accredited certification body, for the purpose of:

- responding to information requests; or
- enabling contact in the event of a complaint about a certification.

b. maintaining an application process for the purpose of:

- information on the status of an application; or

- evaluations by the Malta SA with respect to feedback and its own decisions.

9.3.2 Communication between the certification body, the Malta SA and the NAB

The certification body shall have a procedure in place to communicate to the Malta SA and the NAB without delay of substantial changes that may affect its ability to conform with the accreditation requirements. Such substantial changes may include:

a. a change in its legal, commercial, organizational or ownership status;

b. a change in the organisation's senior management and key staff; and, or

c. a change in its financial resources.

9.3.3 Documentation of evaluation activities

Systems shall be in place for implementing appropriate procedures and communication structures between the certification body and the Malta SA. This shall include a reporting framework to inform the Malta SA:

a. of details of applicant on receipt of application to enable the Malta SA to check its records for the applicant's compliance history as per section 7(6) of this document; and

b. of the reasons for granting/withdrawing certification pursuant to Article 43(5) GDPR immediately prior to issuing, renewing, suspending or withdrawing certifications as per section 7(1)(c) of this document.

9.3.4 Management of complaint handling

A complaint handling procedure shall be established as an integral part of the management system, which shall in particular implement the requirements of sub-clauses 4(1)(2)(2)(c), 4(1)(2)(2)(j), 4(6)(d) and clause 7(13) of ISO 17065.

Relevant complaints and objections shall be shared with the Malta SA.

9.3.5 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 notification of clients.