DATA PROTECTION AUTHORITY

Athens, 06-08-2020

Ref. No. Γ/ΕΞ/5511/06-08-2020

DESCISION 25/2020

The Data Protection Authority met, at the invitation of its President, at a regular meeting at its headquarters on Wednesday 05.08.2020, following the 22.07.2020 meeting, in order to examine the issue concerning the maintenance or modification of the draft decision of the additional requirements for the accreditation of bodies granting certifications to controllers and processors in accordance with Articles 42 and 43 of Regulation (EU) 2016/679 for the protection of individuals with regard to the processing of personal data (GDPR) following the Opinion 22/2020 adopted by the European Data Protection Board. […]

The Authority took into account the following:

By decision no. 8/2020 the Authority decided to draw up a draft setting out the additional requirements, in relation to EN-ISO/IEC 17065/2012, for the accreditation of certification bodies as provided for in Articles 43(1)(b), 43(3) and 57(1) of the GDPR as well as Article 37(1) of Law 4624/2019. Prior to the adoption of this draft decision, the Authority implemented the consistency mechanism referred to in Article 63 and communicated that draft to the European Data Protection Board in accordance with Article 64(1)(c) of the GDPR. The Board, following a written procedure, provided for in Article 24(3) of its Rules of Procedure, which was completed on 23 July 2020, adopted Opinion 22/2020 on the Authority's draft decision on the basis of Article 64(3) of the GDPR. In that opinion, sent to the Authority by electronic means on 29 July 2020, the Board requested the Authority to amend its draft decision on the basis of the recommendations included in the opinion in order that a consistent implementation of

accreditation of certification bodies may be achieved.

The Authority, after hearing the Rapporteurs and Assistant Rapporteurs, who subsequently left, and after a thorough discussion

CONSIDERED IN ACCORDANCE WITH THE LAW

1. According to article 9 of Law 4624/2019 -which aims, among other things, to take measures to implement the GDPR- the supervision of the implementation of the provisions of the GDPR in the Hellenic Territory is exercised by the Authority.
2. According to article 15(10) of Law 4624/2019 "*The regulatory acts of the Authority, for which no provision is made for their publication in the Government Gazette, are published on the website of the Authority".*
3. In accordance with Article 43(6) of the GDPR *"The requirements of paragraph 3 of this Article (...) shall be made public by the supervisory authority in an easily accessible form. The supervisory authorities shall also transmit those requirements and criteria to the Board".*
4. In accordance with Article 57(1) (p) of the GDPR, the Authority *"... [shall] draft and publish the requirements for accreditation (...) of a certification body in pursuant to Article 43 (...)"*.
5. In accordance with Article 64(1), (3), (6), (7) and (8) of the GDPR:
   "(paragraph 1) The Board shall issue an opinion where a competent supervisory authority intends to adopt any of the measures below. To that end, the competent supervisory authority shall communicate the draft decision to the Board, when it: (...) c) aims to approve the requirements for accreditation (...) of a certification body pursuant to Article 43 (...)".
   "(paragraph 3) In the cases referred to in paragraphs 1 and 2, the Board shall issue an opinion on the matter submitted to it provided that it has not already issued an opinion on the same matter. That opinion shall be adopted within eight weeks by simple majority of the members of the Board. That period may be extended by a further six weeks, taking into account the complexity of the subject matter. (...)".

"(paragraph 6) The competent supervisory authority referred to in paragraph 1 shall not adopt its draft decision referred to in paragraph 1 within the period referred to in paragraph 3."

"(paragraph 7) The competent supervisory authority referred to in paragraph 1 shall take utmost account of the opinion of the Board and shall, within two weeks after receiving the opinion, communicate to the Chair of the Board by electronic means whether it will maintain or amend its draft decision and, if any, the amended draft decision, using a standardised format."

"(paragraph 8) Where the competent supervisory authority referred to in paragraph 1 informs the Chair of the Board within the period referred to in paragraph 7 of this Article that it does not intend to follow the opinion of the Board, in whole or in part, providing the relevant grounds, Article 65(1) shall apply."

6. In view of the foregoing, the Authority, having taken into account and examined the recommendations and encouragements of the Board included in Opinion 22/2020, considered unanimously that all recommendations and encouragements in that opinion should be accepted, that the necessary changes should be made to the draft additional accreditation requirements which it had originally submitted to the Board and that the amended draft should be communicated to the Board within the deadline referred to in Article 64(7) of the GDPR.
7. To this end, the draft decision of the additional accreditation requirements, set out in decision no. 8/2020 of the Authority, was modified accordingly to comply with all the recommendations and encouragements of Opinion 22/2020 of the Board.

FOR THESE REASONS

The Authority shall decide unanimously to amend the draft additional requirements for accreditation of certification bodies on the basis of the recommendations and encouragements of Board opinion 22/2020 and to communicate the amended draft to the Board in accordance with Article 64(7) of the GDPR. The amended draft decision will be published on the Authority's website in accordance with Articles 43(6) and 57(1) (p) of the GDPR as well as Article 15(10) of Law 4624/2019, after the completion of this procedure.

Accordingly, the amended additional accreditation requirements are set out in the Annex to this decision.

The President	The Secretary
Konstantinos Menoudakos	**Georgia Palaiologou**

Additional Accreditation Requirements of the Hellenic Data Protection Authority for Certification Bodies in Accordance with Articles 43(1)(b) and 43(3) GDPR in Conjunction with ISO/IEC 17065

Table of Contents

Introduction

The establishment of data protection certification mechanisms and of data protection seals and marks is provided for in Article 42 of the GDPR. Establishing these mechanisms can enhance transparency and compliance with the GDPR and allow data subjects to assess the level of data protection of relevant products and services (Recital 100 of the GDPR).

Certification shall be issued by a certification body accredited to this effect, pursuant to Article 43 of the GDPR, to a controller or processor who has submitted the relevant processing operation to the certification mechanism. The accreditation of certification bodies is of particular importance as it provides an authoritative statement of the competence of these bodies that allows the generation of trust in the certification mechanism.

According to Article 37(1) of the implementing Law 4624/2019, the accreditation of bodies issuing certifications, in accordance with Article 42 of the GDPR, is performed by the National Accreditation System (hereinafter E.SY.D.) (www.esyd.gr) with respect to ISO/IEC 17065/2012 (hereinafter ISO 17065) and pursuant to the additional accreditation requirements specified by the Hellenic Data Protection Authority (hereinafter HDPA). In the process of accreditation, the E.SY.D. shall apply these additional requirements in conjunction with ISO 17065.

This document provides the additional accreditation requirements specified by the HDPA with respect to ISO 17065 and in accordance with Articles 43(1)(b) and 43(3) of the GDPR.

These requirements take into account the requirements proposed in the EDPB guidelines 4/2018[1] and shall be read in conjunction with ISO 17065. Section numbers used here correspond to those used in ISO 17065 and the EDPB guidelines. However, certain sections of ISO 17065 are not included in this document. This means that no additional accreditation requirements are specified for these sections but the requirements of each respective section of ISO 17065 are applied.

0. Prefix

This section sets out the terms of cooperation between the HDPA and the E.SY.D. as part of the accreditation of certification bodies. More detailed terms of cooperation, roles, responsibilities and procedures in relation to accreditation will be agreed upon between the HDPA and the E.SY.D.

The E.SY.D. shall inform the HDPA in written form:

1) Of all accreditation requests submitted by certification bodies. In particular, the E.SY.D. shall provide the HDPA with a brief description of the request, the name and contact details of the certification body, the certification scheme for which accreditation is requested and whether the certification criteria are approved by the competent

[1] *'Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation (2016/679)'*
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_4_2018_accreditation_en.pdf

supervisory authority or the EDPB. In case the accreditation application is submitted to the E.SY.D. before the certification criteria receive the final approval, the E.SY.D. will not grant the accreditation until the certification criteria receive the final approval.

2) Of the reasons for granting or revoking accreditation before granting or revoking accreditation. Information provided to the HDPA shall include, as a minimum, information on the name and contact details of the certification body, the period during which accreditation has been granted, the date of the initial accreditation, the start and end dates of the current accreditation, as well as the certification scheme related to the accreditation.

3) Of the actions taken to revoke accreditation in the event that the E.SY.D. is informed by the HDPA that the accreditation requirements are no longer met, or the certification body is in breach of the GDPR and the provisions of Law 4624/2019 (Article 37(2) of Law 4624/2019).

The HDPA, if it deems appropriate, shall inform the E.SY.D. within a reasonable time of any important reasons for non-compliance by the certification body with the GDPR. Although the E.SY.D. can continue the accreditation process, it shall not conclude it until the HDPA has reached its final decision in this respect. Although the E.SY.D. is free to decide with regard to the granting of accreditation, the E.SY.D. should take into account the final decision taken by the HDPA, without prejudice to the power of the HDPA to revoke it afterwards, if appropriate.

Information provided by the HDPA to the E.SY.D. as part of the accreditation process shall be kept confidential.

The E.SY.D. shall allow full transparency to the HDPA with respect to the accreditation process in accordance with Articles 43(4) and (7), 58(1)(b) of the GDPR and Article 37(2) of Law 4624/2019.

The personnel of E.SY.D. that is responsible for evaluations and is involved in the accreditation process of certification bodies shall be able to demonstrate knowledge with regard to the GDPR and the protection of personal data.

1. Scope

This document contains the additional accreditation requirements of the HDPA to ISO 17065 in accordance with Articles 43(1)(b) and 43(3) of the GDPR and taking into account the EDPB guidelines 4/2018.

The scope of ISO 17065 shall be applied in accordance with the GDPR. The EDPB guidelines 4/2018 on accreditation and the guidelines 1/2018 on certification provide further information. The broad scope of ISO 17065 covering products, processes and services should not lower or override the requirements of the GDPR, e.g. a governance mechanism cannot be the only element of a certification mechanism, as the certification must include processing of personal data, i.e. the processing operations.

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

Pursuant to Article 42(1) of the GDPR, GDPR certification is only applicable to the processing operations of controllers and processors.

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 (EDPB 4/2018) and certification (EDPB 1/2018) shall apply and have precedence over ISO definitions.

To facilitate a common understanding the main definitions are set out below:

- '*GRPR*': Regulation 2016/679/EC - General Data Protection Regulation.
- '*ISO 17065*': ISO/IEC 17065/2012.
- *'Certification'*: The assessment and impartial, third-party attestation that the fulfillment of the certification criteria has been demonstrated in the context of certification under Articles 42 and 43 of the GDPR with respect to processing operations by controllers and processors.
- *'Accreditation'*: Third-party attestation related to the activities of a conformity assessment body conveying formal demonstration of its competence to carry out certification pursuant to Articles 42 and 43 of the GDPR. This is the result of the assessment process for a successful certification body (as part of the accreditation process).
- '*Certification body'*: Third-party conformity assessment body operating certification schemes.
- '*Certification criteria*': The criteria against which a certification is performed for a given certification scheme.
- *'Certification scheme'*: A certification system related to specified products, processes and services to which the same requirements, rules and procedures apply. It mainly includes the certification criteria and assessment methodology.
- '*Certification mechanism'*: The system by which a controller or processor becomes certified. It is an approved certification scheme which is available to the applicant with a set of existing procedures. It is a service provided by an accredited certification body based on approved criteria and assessment methodology.

- *'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 controller or processor that has applied for certification of their processing operations

- *'Client'*: The controller or processor that has been certified.

4. General requirements for accreditation

4.1 Legal and contractual matters

4.1.1 Legal responsibility

Certification bodies shall be able to demonstrate (at all times) to the E.SY.D. 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.

As the certification body is a data controller/processor itself, it shall be able to demonstrate evidence of the GDPR and Law 4624/2019 compliant procedures and measures specifically for controlling and handling of client organisation's personal data as part of the certification process.

The certification body shall:

- be able to demonstrate evidence of the GDPR compliance at any time during the accreditation process;

- inform the E.SY.D. of any infringements of the GDPR or Law 4624/2019established by the HDPA and/or judicial authorities which can affect accreditation;

- allow full transparency to the HDPA with respect to the accreditation and certification procedures in accordance with Articles 42(7), 43(4) of the GDPR, 58(1)(b) and (c) of the GDPR and Article 37(2) of Law 4624/2019.

4.1.2 Certification agreement ('CA')

In addition to point 4.1.2.1 of ISO 17065, the legally enforceable agreement shall be in written form. The certification body shall demonstrate, in addition to the relevant 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) of ISO 17065 and the

certification criteria approved by the HDPA or the EDPB in accordance with Articles 43(2)(b) and 42(5) of the GDPR;

2. require the applicant to allow full transparency to the HDPA with respect to the certification procedure, including contractually confidential matters 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 GDPR and are without prejudice to the tasks and powers of the HDPA 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) 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 HDPA all information necessary for the granting or withdrawal of the certification and the reasons for the relevant decision pursuant to Articles 42(8) and 43(5) of the GDPR;

8. include rules on the necessary precautions for the investigation of complaints, within the meaning of 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 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 shall also be addressed by including appropriate procedures into 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. require the applicant to inform the certification body of any infringements of the GDPR established by the HDPA and/or judicial authorities that may affect certification;

12. set out the terms and conditions defining the duration of the certification procedure and 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 GDPR and the guidelines on accreditation and certification.

4.2 Management of impartiality

The E.SY.D. shall ensure, in addition to the requirements in 4.2 of ISO 17065, that:

1. the certification body shall comply with the additional requirements of the HDPA (pursuant to Article 43(1)(b) of the GDPR)

    a. in line with Article 43(2)(a) of the GDPR shall 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. the certification body shall provide separate evidence that its tasks and obligations do not lead to a conflict of interest pursuant to Article 43(2)(e) of the GDPR.
    c.
2. the certification body has no relevant connection with the client it assesses. The certification body should not belong to the same company group nor should be controlled in any way by the client it assesses.

The certification body shall ensure that there are no conflicts of interest and shall be able to demonstrate on a regular basis, that it carries out its conformity assessment activities impartially, does not allow commercial, financial or other pressures to compromise impartiality and manages any conflicts of interest that may be identified.

4.3 Liability and financing

The E.SY.D. shall, in addition to the requirements in 4.3.1 of ISO 17065, ensure on a regular basis that the certification body:

1. has evaluated the risks related to its certification activities and has appropriate measures (e.g. insurance or reserves) to cover its liabilities arising from its operations and fields of activities in the geographical regions in which it operates, and

2. can adequately demonstrate its financial stability and resources required for its operations.

4.6 Publicly available information

The E.SY.D. shall, in addition to the requirement in 4.6 of ISO 17065, require from the certification body that at minimum

1. all versions (current and previous) of the approved criteria used within the meaning of Article 42(5) of the GDPR are published and made 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, Article 43(4) of the GDPR ["proper" assessment]

5.1 Organisational structure and top management

The E.SY.D. shall, in addition to the requirements in 5.1.3 of ISO 17065, require from the certification body to appoint a person with overall authority and responsibility for overseeing data protection certification evaluation, decisions and supervision.

6. Resource requirements

6.1 Certification body personnel

The E.SY.D. shall, in addition to the requirement in section 6 of ISO/IEC 17065, ensure for each certification body that its personnel:

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

2. has independence and ongoing expertise with regard to the ToE 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) of the GDPR 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 the these additional requirements, specifically

For personnel with *technical expertise:*

- Must have obtained a degree in information technology, computer science or mathematics of at least EQF level 6 from a Greek or a foreign university, or an equivalent vocational education enjoying a recognized protected title in the Member State where it was issued. The degree from the foreign university must be recognized by the state. In addition, must have obtained the academic degree Master or equivalent, and have relevant professional experience.
- *Personnel responsible for certification decisions* shall demonstrate at least two years professional and comprehensive experience and expertise in identifying and implementing data protection measures.
- *Personnel responsible for evaluations* shall demonstrate at least two years professional experience in technical data protection and knowledge, specialist expertise and professional experience in technical procedures (e.g. audits and certifications).

For personnel with *legal expertise*:

- Must have obtained a degree in law from a Greek or a foreign university. The degree in law from the foreign university must be recognized by the state. In addition, must have obtained an academic Master's degree (LL.M.) or equivalent, and have relevant professional experience.
- *Personnel responsible for certification decisions* shall demonstrate at least two years professional and comprehensive experience and expertise in certification measures related to data protection law.
- *Personnel responsible for evaluations* shall demonstrate at least two years of professional experience in data protection law and knowledge, specialist expertise and professional experience in technical procedures (e.g. audits and certifications).

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

6.2 Resources for evaluation

The certification body, in addition to the requirements of section 6.2 of ISO 17065, shall demonstrate that the conditions in point 6.1 of these requirements apply to personnel of bodies that the certification body has outsourced evaluation activities.

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

7.1 General

The E.SY.D. shall, in addition to the requirements in section 7.1 of ISO 17065, ensure the following:

1. that certification bodies comply with the additional requirements of the HDPA (pursuant to Article 43(1)(b) of the GDPR) in order that tasks and obligations do not lead to a conflict of interests pursuant to Article 43(2)(b) of the GDPR;

2. notify the relevant competent supervisory authorities before a certification body starts operating an approved European Data Protection Seal in a new Member State from a satellite office;

3. that certification bodies have established procedures to examine that the procedures and mechanisms of the applicant for processing and handling personal data related to the scope of the certification and the ToE are compliant with the GDPR;

4. that certification bodies have established procedures/mechanisms to inform the HDPA in written form before granting**,** extending, renewing or withdrawing/revoking the requested certification. The certification body shall provide to the HDPA the reasons for the relevant decision and a copy of the executive summary of the evaluation report mentioned in section 7.8 (also including the following information: name of the client, description of the ToE of the certification and a short public assessment);

5. that certification bodies have established procedures to investigate and respond in written form without undue delay to any requests made by the HDPA regarding the provision of aggregate data for certifications, among other things, and complaints submitted, as well as of details on specific cases.

7.2 Application

In addition to item 7.2 of ISO 17065, it shall be required that:

1. the ToE must be described in detail in the application. This also includes interfaces and transfers to other systems and organizations, protocols and other assurances;

2. the application shall specify whether processors are used, and when processors are the applicant, their responsibilities and tasks shall be described, and the application shall contain the relevant controller/processor contract(s);

3. the application shall specify 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 agreed arrangements.

At the application stage the certification body shall be required to provide to the HDPA a short description of each one of the applications.

7.3 Application review

In addition to item 7.3 of ISO 17065, it shall be required that:

1. binding evaluation methods with respect to the ToE shall be laid down in the certification agreement;
2. the assessment in 7.3.1 (e) and 7.3.3 of ISO 17065 takes into account both technical and legal expertise in data protection to an appropriate extent;
3. the application review shall consider all the information referred to in point 7.2 of these requirements.

7.4 Evaluation

In addition to item 7.4 of ISO 17065, the 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 organizational measures pursuant to Articles 24, 25 and 32 of the GDPR, insofar as the aforementioned Articles apply to the ToE, 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 ToE 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 standardised and generally applicable. 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, it shall be allowed that the evaluation is carried out by external experts who have been recognised by the certification body. The same personnel requirements described in section 6 of these requirements apply to these external experts.

In addition to item 7.4.5 of ISO 17065, it shall be provided that existing data protection certification in accordance with Articles 42 and 43 of the GDPR, which already covers

part of the ToE, may be included in a current certification. However, it will not be sufficient to completely replace (partial) evaluations. The certification body shall be obliged to check the compliance with the criteria in respect of the ToE. Recognition shall in any way require the preparation of a complete evaluation report or information enabling an evaluation of the existing certification and its results. A certification statement or similar certification certificates shall not be considered sufficient to replace a report.

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 applicant about non-conformities from the scheme. In this context, at least the nature and timing of such information shall be defined.

In addition to item 7.4.9 of ISO 17065, it shall be required that documentation be made fully accessible to the HDPA upon request.

7.5Review

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

In addition to point 7.5.1 of ISO 17065, the certification body shall demonstrate how the person(s) assigned to review have not directly nor indirectly been involved in the evaluation process.

7.6Certification decision

In addition to point 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.

The certification body shall inform the HDPA in written form before issuing its certification decision and shall provide the reasons for the relevant decision.

In addition to point 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.

7.7Certification 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 of the present requirements is documented.

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

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 shall 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 shall explain such things as:

(a) the name and contact details of the client,

(b) the scope of the certification and a meaningful description of the ToE,

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

(d) the evaluation methods and tests conducted,

(e) the result(s),

(f) the date of granting and the data of expiration of the current certification and

(g) the initial and all re-certification dates.

In addition to item 7.8 of ISO 17065 and pursuant to Article 43(5) of the GDPR, the certification body shall inform the HDPA 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 GDPR, regular monitoring measures are required to maintain certification during the monitoring period. Such measures should be risk based and proportionate and surveillance activities should be performed at least twice during the certification cycle.

The type and regularity of surveillance activities shall be determined in the certification scheme.

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:

- 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 and documents adopted by the EDPB and
- court decisions related to data protection.

The above changes also include the case in which the state of the art, which was valid at the time of certification and had been taken into account in order to grant certification, has now become obsolete in the light of recent technological developments.

The change procedures to be implemented by the certification body shall include such things as: transition periods, approvals process with the HDPA, 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 item 7.11.1 of ISO 17065, the certification body shall be required to inform the HDPA and the E.SY.D. immediately in written form 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 HDPA 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 HDPA that proper action has been taken.

Serious data breach incidents relating to the scope of the certification and the ToE should be considered as non-compliance with the certification, and appropriate actions should be taken by the certification body. The certification body shall inform the HDPA immediately in written form about such actions. Such requirement does not affect the obligation of the client to inform the HDPA about data breaches in accordance to the provisions of the GDPR.

7.12 Records

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

In addition to items 7.10 and 7.12 of ISO 17065, the certification body shall maintain a record of all the changes affecting the certification, the actions taken to implement changes and the status of the certification.

The contact details of the certification body personnel that is responsible for evaluations and certification decisions shall be kept in a record file separately for each certification case and be made available to the HDPA if requested. The purpose of this requirement is to allow the HDPA, when needed, to verify that the personnel responsible for evaluations are different from the personnel responsible for the certification decisions for each certification case (i.e. separation of duties).

7.13 Complaints and appeals, Article 43(2)(d) of the GDPR

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.

In addition to items 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.

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.

The certification bodies shall make the complaints handling procedure easily publicly available.

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.

These management principles and their documented implementation must be transparent and be disclosed by the accredited certification body pursuant in the accreditation procedure pursuant to Article 58 and at the request of the HDPA at any time during an investigation in the form of data protection reviews pursuant to Art. 58(1)(b) of the GDPR or a review of the certifications issued in accordance with Article 42(7) of the GDPR 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), how long the certifications are valid under which framework and conditions (recital 100 of the GDPR).

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 the present requirements. 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 the present requirements.

9.3 Responsibilities and competencies

9.3.1 Communication between CB and its applicants and clients

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

1. Maintaining documentation of tasks and responsibilities by the accredited certification body, for the purpose of

    a. Information requests, or

b. To enable contact in the event of a complaint about a certification.

2. Maintaining an application process for the purpose of

a. Information on the status of an application;

b. Evaluations by the HDPA with respect to

i. Feedback;

ii. Decisions by the HDPA.

9.3.3 Management of complaint handling

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

Relevant complaints and objections shall be shared with the HDPA.

9.3.4 Management of withdrawal

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