DECISION no. 20 of 24th of June 2021
on the additional requirements for the accreditation of certification bodies pursuant to Article 43 of Regulation (EU) 2016/679

Considering the provisions of Article 42 paragraph (1) of 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), hereinafter referred to as the General Data protection Regulation,

Considering the provisions of Article 43 of the General Data Protection Regulation on the certification bodies which provides that Member States shall ensure that certification bodies may be accredited by the national accreditation body designated in accordance with 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, in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the national supervisory authority which is competent pursuant to Article 55 or 56 of the General Data Protection Regulation,

Having regard to the official quality of the Romanian Accreditation Association – RENAR as a national accreditation body, pursuant to Regulation (EC) no. 765/2008 and of the Government Ordinance no. 23/2009 on the accreditation activity of the bodies for the conformity assessment, approved with amendments through Law no. 256/2011, as well as of the Law no. 190/2018 on implementing measures to 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), with subsequent amendments,

Considering the European Standard EN-ISO/IEC 17065/2012 (Romanian Standard SR EN ISO/IEC 17065:2013 is identical to the European Standard EN-ISO/IEC 17065/2012 and has the same status as the official versions, being published with the permission of the Joint European Standardisation Organisation),

Having regard to the document issued by the European Data Protection Board entitled "*Guidelines 1/2018 on certification and identifying certification criteria in accordance with*

Articles 42 and 43 of the General Data Protection Regulation", version 3.0 of the 4th of June 2019,

Taking into account the fact that the Romanian certification body – RENAR was consulted by the national supervisory authority on the draft document containing the Additional requirements for the accreditation of certification bodies pursuant to Article 43 of Regulation (EU) 2016/679,

Taking into account Article 64 (1) letter c) of the General Data Protection Regulation, according to which the European Data Protection Board issues an opinion each time a competent supervisory authority intends to approve requirements for the accreditation of a certification body in accordance with Article 43 (3) or the certification criteria mentioned in Article 42 (5) of the General Data Protection Regulation,

Considering the Opinion no. 13 of 23rd of March 2021 of the European Data Protection Boards, according to which the European Data protection Board issues an opinion each time a competent supervisory authority intends to approve requirements for the accreditation of certification bodies pursuant to Article 43 of Regulation (EU) 2016/679,

Based on the note of the Legal and Communication Department no. 125 of 7th of August 2020 on the draft Decision regarding the "additional requirements for the accreditation of certification bodies pursuant to Article 43 of Regulation (EU) 2016/679",

Based on the provisions of Article 3 (5) and (6) and of Article 10 (1) letters a) and b) of Law no. 102/2005 on the set up, organisation and functioning of the National Supervisory Authority for Personal Data Processing – republished, as well as those of Article 6 (2) letter b) of the Regulation on the organisation and functioning of the National Supervisory Authority for Personal Data Processing, approved by Decision no. 16/2005 of Standing Bureau of the Senate, with the subsequent amendments and completions,

the president of the National Supervisory Authority for Personal Data Processing issues this decision.

Article 1

The Requirements on the additional requirements for the accreditation of certification bodies pursuant to Article 43 of Regulation (EU) 2016/679, provided in the annex which is an integral part of this decision, are approved.

Article 2

This decision enters into force on the date of publication in the Official Journal of Romania, Part I.

President of the National Supervisory Authority for Personal Data Processing,

Ancuţa Gianina Opre

ANNEX

Additional requirements for the accreditation of certification bodies pursuant to Article 43 of Regulation (EU) 2016/679

Chapter I: INTRODUCTION

Regulation (EU) 2016/679 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) provides that the Member States, the data protection supervisory authorities, the Board and the European Commission encourages the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors, by taking into account the specific necessities of micro, small and medium-sized enterprises.

Correlated with these provisions, Article 43 of Regulation (EU) 2016/679 provides that Member States shall ensure that certification bodies may be accredited by the national accreditation body named in accordance with Regulation (EC) No 765/2008 of the European Parliament and of the Council in accordance with EN-ISO/IEC 17065/2012 and with the additional requirements established by the data protection supervisory authority.

At the level of the National Authority for the Supervision of Personal Data Processing (hereinafter ANSPDCP), this document was elaborated, which contains “Additional requirements for the accreditation of certification bodies pursuant to Article 43 of Regulation (EU) 2016/679”.

When drafting the document containing the additional requirements, a series of documents were taken into account, including the requirements EN-ISO/IEC 17065/2012 and Guidelines 1/2018 on certification and identifying certification criteria, document adopted by the European Data Protection Board.

The European standard EN-ISO/IEC 17065/2012 is identical to the Romanian standard SR EN ISO/CEI 17065:2013.

SR EN ISO/CEI 17065:2013 represents the Romanian version of the English text of the European standard EN-ISO/IEC 17065/2012 which was translated by ASRO (Romanian National Standardization Body), has the same status as the official versions and was published with permission from CEN (Common European Standardization Organization).

Also, considering the official quality of the Romanian Accreditation Association – RENAR as a national accreditation body, pursuant to Regulation (EC) no. 765/2008 and G.O. no. 23/2009 on the accreditation activity of the bodies for the conformity assessment, approved with amendments through Law no. 256/2011, it was consulted on the content of the document entitled "Additional requirements for the accreditation of certification bodies pursuant to Article 43 of Regulation (EU) 2016/679".

CHAPTER II: SCOPE

This document contains additional requirements to EN-ISO/IEC 17065/2012 for assessing the competence, consistent operation and impartiality of data protection certification bodies.

The scope of EN-ISO/IEC 17065/2012 shall be applied in accordance with Regulation (EU) 2016/679. The guidelines on accreditation and certification provide further information. The scope of a certification mechanism (for example, certification of cloud service processing operations) shall be taken into account in the assessment by the RENAR and ANSPDCP during the accreditation process, particularly with respect to criteria, expertise and evaluation methodology. The broad scope of EN-ISO/IEC 17065/2012 covering products, processes and services shall 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. Pursuant to Article 42 paragraph (1) from Regulation (EU) 2016/679, the certification is only applicable to the processing operations of controllers and processors

CHAPTER III: DEFINITIONS

In the context of this document, the terms and definitions of the guidelines on accreditation (European Data Protection Board Guidelines 4/2018) and certification (European Data Protection Board Guidelines 1/2018) shall apply and have precedence over the definitions offered by EN-ISO/IEC 17065/2012.

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

- *Certification*: The assessment and impartial, third-party attestation that the fulfilment of the certification criteria has been demonstrated in the context of certification under Articles 42 and 43 of Regulation (EU) 2016/679 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 Regulation (EU) 2016/679. 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 organisation that has applied for certification of their processing operations.
- *Client*: The organisation that has been certified.

CHAPTER IV: GENERAL REQUIREMENTS FOR ACCREDITATION

Section 1: 4.1. Legal and contractual matters

4.1.1 Legal responsibility

A certification body shall be able to demonstrate (at all times) to the Romanian Accreditation Association – RENAR 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 Regulation (EU) 2016/679. Note that, as the certification body is a data controller/processor itself, it shall be able to demonstrate evidence of Regulation (EU) 2016/679 compliant procedures and measures specifically for controlling and handling of client organisation's personal data as part of the certification process.

ANSPDCP 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 EN-ISO/IEC 17065/2012 that its certification agreement (the contract between the certification body and the client):

1. requires the applicant to always comply with both the general certification requirements within the meaning of 4.1.2.2 letter a) EN-ISO/IEC 17065/2012 and the criteria approved by ANSPDCP or the European Data Protection Board in accordance with Article 43 (2)(b) and Article 42(5) of Regulation (EU) 2016/679;
2. requires the applicant to allow full transparency to ANSPDCP 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 Regulation (EU) 2016/679;
3. does not reduce the responsibility of the applicant for compliance with Regulation (EU) 2016/679 and is without prejudice to the tasks and powers of ANSPDCP which is competent in line with Article 42 paragraph (5) of Regulation (EU) 2016/679;
4. requires 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 paragraph (6) of Regulation (EU) 2016/679;
5. requires 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. sets out the rules of validity, renewal and withdrawal pursuant to Articles 42 paragraph (7) and 43 paragraph (4) of Regulation (EU) 2016/679, including rules setting appropriate intervals for re-evaluation or review (regularity) in line with Article 42 paragraph (7) of Regulation (EU) 2016/679;

7. allows the certification body to disclose all information necessary for granting certification pursuant to Articles 42 paragraph (8) and 43 paragraph (5) of Regulation (EU) 2016/679;

8. includes rules on the necessary precautions for the investigation of complaints; additionally, shall also contain explicit statements on the structure and the procedure for complaint management in accordance with Article 43 paragraph (2) letter (d) of Regulation (EU) 2016/679;

9. establishes the consequences for the client of the certification body in the situation where the accreditation of the certification body was suspended or withdrawn and this has an impact on the client, as well as the steps that shall be taken;

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

4.1.3 Use of data protection seals and marks

Certificates, seals and marks shall only be used in compliance with Article 42 and 43 of Regulation (EU) 2016/679 and the guidelines on accreditation and certification.

A copy of the seal/mark/logo shall be provided to ANSPDCP.

Section 2: 4.2. Management of impartiality

The accreditation body (RENAR) shall ensure that in addition to the requirement in 4.2. of EN-ISO/IEC 17065/2012,

1. the certification body comply with the additional requirements of ANSPDCP [pursuant to Article 43(1)(b) of Regulation (EU) 2016/679]

a. in line with Article 43(2)(a) of Regulation (EU) 2016/679 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;

b. its tasks and obligations do not lead to a conflict of interest pursuant to Article 43(2)(e) of Regulation (EU) 2016/679;

2. the certification body has no relevant connection with the client it assesses, e.g. the certification body should not belong to the same company group nor should be controlled in any way by the client it assesses.

Section 3: 4.3. Liability and financing

The accreditation body (RENAR) shall in addition to the requirement in 4.3.1 of EN-ISO/IEC 17065/2012 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.

The certification body shall demonstrate its financial stability and independence. The certification body shall have civil liability insurance appropriate to the field of activity. The amount of liability insurance shall be determined on the basis of the results of the assessment of the risks arising from its activities.

Section 4: 4.4. Non-discriminatory conditions

The requirements of EN-ISO/IEC 17065/2012 shall apply.

Section 5: 4.5. Confidentiality

The requirements of EN-ISO/IEC 17065/2012 shall apply.

Section 6: 4.6. Publicly available information

The accreditation body (RENAR) shall in addition to the requirement in 4.6 of EN-ISO/IEC 17065/2012 require from the certification body that at minimum:

1. all versions (current and previous) of the approved criteria used in the meaning of Article 42(5) of Regulation (EU) 2016/679 are published and easily publicly available as well as all certification procedures, generally stating the respective period of validity. The form of publication shall be appropriate to inform the public in the most comprehensive way possible. This is usually guaranteed by the electronic form.

2. information about complaints handling procedures and appeals are made public pursuant to Article 43(2)(d) of Regulation (EU) 2016/679. At the same time, this obligation to

publish refers not only to particular incidents, but also to the structure and procedure for handling complaints by the certification body. The information that is made public refers only to statistics or other type of anonymised information.

CHAPTER V: STRUCTURAL REQUIREMENTS

Section 1: 5.1. Organisational structure and top management

The requirements of EN-ISO/IEC 17065/2012 shall apply.

Section 2: 5.2. Mechanism for safeguarding impartiality

In addition, according to Chapter 5 (chapters 5.1.1 and 5.2) of EN-ISO/IEC 17065/2012, the certification body shall demonstrate to the RO SA, within the accreditation procedure, that the assurance mechanism of independence meets the requirements of Article 43(2)(a) and (e) of Regulation (EU) 2016/679 and that its tasks and obligations do not lead to a conflict of interests. Independence means that the certification body in question can act without instructions and pressure, and financial stability is ensured.

CHAPTER VI: RESOURCE REQUIREMENTS

Section 1: 6.1. Certification body personnel

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

1. has demonstrated appropriate and ongoing expertise (knowledge and experience) with regard to data protection pursuant to Article 43(1) of Regulation (EU) 2016/679;
2. has independence and ongoing expertise with regard to the object of certification pursuant to Article 43(2)(a) of Regulation (EU) 2016/679 and do not have a conflict of interest pursuant to Article 43(2)(e) of Regulation (EU) 2016/679;
3. undertakes to respect the criteria referred to in Article 42(5) pursuant to Article 43(2)(b) of Regulation (EU) 2016/679;
4. has relevant and appropriate knowledge about and experience in applying data protection legislation;

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

6. is able to demonstrate experience in the fields mentioned in the additional requirements provided under points 1, 4 and 5.

(2) For personnel with technical expertise:

- have obtained a qualification in a relevant area of technical expertise to at least CEC[1] level 6 or a recognised protected title (e.g. proof of experience, previous contracts, attestation by previous employers) in the relevant regulated profession or have significant professional experience.

- *Personnel responsible for certification decisions* require significant professional experience in identifying and implementing data protection measures; this may be evidenced by documents relating to appropriate professional qualifications, courses, etc attesting to the qualifications or competencies required.

- *Personnel responsible for evaluations* shall demonstrate at least two years of professional experience in data protection, as well as technical knowledge and experience in comparable procedure (e.g. certifications/audits, proof of experience, previous contracts, attestation by previous employers); this may be evidenced by documents relating to appropriate professional qualifications, courses, etc., attesting to the qualifications or competencies required.

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

(3) For personnel with legal expertise:

- to have 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.

- *Personnel responsible for certification decisions* shall demonstrate significant professional experience in data protection field; this may be evidenced by documents relating to appropriate professional qualifications, courses, etc., attesting to the qualifications or competencies required.

- *Personnel responsible for evaluations* shall demonstrate at least two years of professional experience in data protection fields and knowledge and experience in comparable procedures (e.g. certifications/audits, proof of experience, previous contracts, attestation by

[1] Please see the comparison instrument of the qualifications frameworks at the address https://ec.europa.eu/ploteus/ro/compare

previous employers); this may be evidenced by documents relating to appropriate professional qualifications, courses, etc., attesting to the qualifications or competencies required.

Personnel shall demonstrate they maintain domain specific knowledge in the field (technical and/or legal competences), as well as audit skills through continuous professional development.

Section 2: 6.2. Resources for evaluation

The requirements of EN-ISO/IEC 17065/2012 shall apply.

CHAPTER VII: PROCESS REQUIREMENTS

Section 1: 7.1. General

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

1. certification bodies comply with the additional requirements of the sompetent supervisory authority [pursuant to Article 43(1)(b) of Regulation (EU) 2016/679] when submitting the application in order that tasks and obligations do not lead to a conflict of interests pursuant to Article 43(2)(b) of Regulation (EU) 2016/679;
2. notify the relevant competent data protection supervisory authorities before a certification body starts operating an approved European Data Protection Seal in a new Member State from a satellite office.

Section 2: 7.2. Application

In addition to item 7.2 of EN-ISO/IEC 17065/2012, the target of evaluation (ToE) must be described in detail in the application. This also includes interfaces and transfers to other systems and organizations, protocols and other assurances. Also, 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).

Furthermore, 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.

The controller and the processor have the right to apply for certification, having regard that the possibility for the processors to be certified will depend on the scope of the certification scheme.

Section 3: 7.3. Application review

In addition to chapter 7.3 of EN-ISO/IEC 17065/2012, binding evaluation methods with respect to the target of evaluation and taking into account the data protection law applicable to the client shall be laid down in the certification agreement. At the same time, the assessment in 7.3(e) of whether there is sufficient expertise shall take into account both technical and legal expertise in data protection to an appropriate extent.

Section 4: 7.4. Evaluation

(1) In addition to chapter 7.4 of ISO/IEC 17065/2012, certification mechanisms shall describe sufficient evaluation methods for assessing the compliance of the processing operation(s) with the certification criteria, including for example where applicable:

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

2. a method for 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 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 criteria are met; and

4. documentation of methods and findings.

(2) The certification body shall be required to ensure that these evaluation methods are standardized and generally applicable. This means that comparable evaluation methods are

used for comparable certification domains (including objects of certification). Any deviation from this procedure shall be justified by the certification body.

(3) In addition to item 7.4.2 of EN-ISO/IEC 17065/2012, it should be allowed that the evaluation is carried out by external experts who have been recognized by the certification body. Also, the certification body will retain the responsibility for the decision-making, even when it uses external experts.

(4) In addition to item 7.4.5 of EN-ISO/IEC 17065/2012, it shall be required that data protection certification in accordance with Articles 42 and 43 of Regulation (EU) 2016/679, which already covers part of the object of certification, may be included in a current certification. However, it will not be sufficient to completely replace (partial) evaluations. The certification body shall be obliged to check the compliance with the criteria. Recognition shall in any way require the availability of a complete evaluation report or information enabling an evaluation of the existing certification and its results. A certification statement or similar certification certificates shall not be considered sufficient to replace a report.

(5) Existing certifications may be considered in particular as follows:

1. Data protection certification in accordance with Article 42 of Regulation (EU) 2016/679, where the parts of the certification object have already been certified by an accredited certification body, may be considered to be a partial evaluation.

2. However, the data protection certifications pursuant to Article 42 of Regulation (EU) 2016/679 are not acceptable to completely replace the (partial) evaluations. The certification body continues to be required to verify the current compliance with the requirements (certification submitted), at least randomly, and to assess the existing certifications. There are no effects on the period of validity of the certification presented.

3. The period of validity of certificates shall be documented and kept available in accordance with chapter 7.7 of EN-ISO/IEC 17065/2012.

(6) In addition to chapter 7.4.6 of EN-ISO/IEC 17065/2012, it shall be required that the certification body shall set out in detail in its certification mechanism how the information required in chapter 7.4.6 informs the client (certification applicant) about nonconformities from a certification mechanism. In this context, at least the nature and timing of such information shall be defined.

(7) In addition to chapter 7.4.9 of EN-ISO/IEC 17065/2012, it shall be required that documentation be made fully accessible to the data protection supervisory authority upon request.

The documentation must be fully accessible during the accreditation procedure and at all times, at the request of the data protection supervisory authority.

Section 5: 7.5. Review

In addition to chapter 7.5 of EN-ISO/IEC 17065/2012, procedures for the granting, regular review and revocation of the respective certifications pursuant to Article 43(2) and 43(3) are required.

Section 6: Chapter 7.6. Certification decision

In addition to chapter 7.6.1 of EN-ISO/IEC 17065/2012, the certification body shall be required to set out in detail in its procedures how its independence and responsibility with regard to individual certification decisions are ensured.

In addition to chapter 7.6.1 of EN-ISO/IEC 17065/2012, the certification body must specify in detail its criteria, how independence and accountability for certification decisions are ensured.

In accordance with chapter 7.8 of EN-ISO/IEC 17065/2012, the certification body shall publish a brief public assessment of the result of the certification.

The certification body shall inform ANSPDCP, in written, about the certification. The written information must include the name of the client, a description of the object of certification and a brief public assessment. This activity to inform ANSPDCP is for transparency purposes and does not imply actions from ANSPDCP.

In addition to chapter 7.6.2 of EN-ISO/IEC 17065/2012, the decision on certification must be taken by the head of the certification body or a qualified person directly appointed by him. In this respect, chapter 7.6.3 of EN-ISO/IEC 17065/2012 must be observed. The assessment may be performed by experts, previously recognized by the certification body, as described in addition to chapter 7.4.2 of EN-ISO/IEC 17065/2012.

In addition to chapter 7.6.6 of EN-ISO/IEC 17065/2012, the certification body shall specify in its criteria how the client shall be informed about the decision not to grant the certification. In addition, it shall inform the client on the possibility of requesting a reconsideration of the certification body’s decision in the above case and the procedure to be followed by the client.

Section 7: 7.7. Certification documentation

In addition to chapter 7.7.1.e of EN-ISO/IEC 17065/2012 and in accordance with Article 42(7) of Regulation (EU) 2016/679, it shall be required that the period of validity of certifications shall not exceed three years.

In addition to chapter 7.7.1.e of EN-ISO/IEC 17065/2012, it shall be required that the period of the intended monitoring within the meaning of section 7.9 of the EN-ISO/IEC 17065/2012will also be documented.

In addition to chapter 7.7.1.f of EN-ISO/IEC 17065/2012, 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).

Chapter 8: 7.8. Directory of certified products

(1) In addition to chapter 7.8 of EN-ISO/IEC 17065/2012, 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 (target of evaluation);

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

(c) the evaluation methods and tests conducted; and

(d) the result(s).

(2) In addition, the information shall include:

1. the contact details of the applicant (legal or natural person),
2. the registration number,
3. the certification date and the expiration date of the certificate,
4. information about the initial certification or recertification,
5. information about possible supervisory activities to maintain certification, and
6. the possible involvement of external evaluators.

(3) In addition to chapter 7.8 of EN-ISO/IEC 17065/2012 and pursuant to Article 43(5) of Regulation (EU) 2016/679, the certification body shall inform the competent data protection supervisory authorities of the reasons for granting or revoking the requested certification.

Section 9: 7.9. Surveillance

In addition to chapters 7.9.1, 7.9.2 and 7.9.3 of EN-ISO/IEC 17065/2012 and according to Article 43(2)(c) of Regulation (EU) 2016/679, it shall be required that regular monitoring measures are obligatory to maintain certification during the monitoring period.

Surveillance must be carried out at least once a year. However, there should be a risk-based approach in order to identify whether, in specific cases, the surveillance activities have to be carried out more than once per year.

The certification procedure and agreement with the client must be demonstrated at all times during the accreditation validity and at the request of the data protection supervisory authorities.

Section 10: 7.10 Changes affecting certification

(1) In addition to chapters 7.10.1 and 7.10.2 of EN-ISO/IEC 17065/2012, changes affecting certification to be considered by the certification body shall include: amendments to data protection legislation or the state of art, the adoption of delegated acts of the European Commission in accordance with Articles 43(8) and 43(9) of Regulation (EU) 2016/679, documents adopted by the European Data Protection Board and court decisions related to data protection. The change procedures could include such things as: transition periods, approvals process with ANSPDCP, reassessment of the object of certification (including object of certification) and appropriate measures to revoke the certification if the certified processing operation is no longer in compliance with the updated criteria.

(2) In addition to chapter 7.10.1 of EN-ISO/IEC 17065/2012, the certification body shall define in its certification scheme:

1. which changes require notification and, where appropriate, a client adjustment,
2. what are the methods of evaluation by the certification body in such a case and
3. what deadlines exist for the implementation of measures to maintain the existing certification.

(3) Beyond this, the certification body defines how it ensures that comparable audits are performed in comparable certification procedures if the certification requires change.

(4) In addition, the certification body also defines what measures and processes must be taken if the audit leads to the conclusion that the certification cannot be maintained. The

appropriate measures and processes shall be implemented and kept by the management of the certification body.

(5) In addition to chapter 7.10.2 of EN-ISO/IES 17065/2012, the certification body shall define in its certification scheme in which cases and in what way the client must provide the certification body with information (in case of changes initiated by the client). This is always the case, at least when there have been changes in the object of certification regarding the processing of personal data, changes in the operational environment and/or changes in the context of the application or change in other framework-conditions that are relevant to the certification statement. This applies in particular to changes in the relevant legal standards regarding the object of certification, as well as changes in the state-of-the-art technology that have been determined by the client. In this case, any measures initiate by notification must be defined by the certification body and the client. The certification body shall also define now to ensure that comparable measures are taken in comparable cases. Also, the certification body has the obligation to take into account the changes notified by the client on the basis of item 7.10.2 of EN-ISO/IES 17065/2012. In addition, appropriate measures and processes shall be implemented and maintained by the management of the certification body.

Section 11: 7.11 Termination, reduction, suspension or withdrawal of certification

In addition to chapter 7.11.1 of EN-ISO/IEC 17065/2012, the certification body shall be required to inform ANSPDCP and the national accreditation body (RENAR) where relevant immediately in writing about measures taken and about continuation, restrictions, suspension and withdrawal of certification.

According to Article 58(2)(h) of Regulation (EU) 2016/679, the certification body shall be required to accept decisions and orders from the competent data protection supervisory authority to withdraw or not to issue certification to a client (applicant) if the requirements for certification are not or no longer met.

Section 12: 7.12. Records

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

This applies to certification procedures completed without a positive result, to certification procedures completed with a positive result and to ongoing certification procedures.

In ongoing certification procedures, the certification criteria that are met and not met must be evident.

In addition, the certification body must keep statistics on finalised and completed procedures.

In addition to chapter 7.12.1 of EN-ISO/IEC 17065/2012, all records relating to the certification process shall be retained for further three years beyond the period of validity of the certification and after the completion of the certification agreement. In the event of a dispute between the certification body and the client or the client and ANSPDCP, this period may be extended beyond the validity period of the certification until the dispute is settled.

Section 13: 7.13 <u>Complaints and appeals</u>

(1) In addition to chapter 7.13.1 of EN-ISO/IEC 17065/2012, 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.

(2) In addition to item 7.13.2 of EN-ISO/IEC 17065/2012, 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.

(3) In addition to chapter 7.13.1 of EN-ISO/IEC 17065/2012, the certification body must define how separation between certification activities and the handling of appeals and complaints is ensured.

CHAPTER VIII: MANAGEMENT SYSTEM REQUIREMENTS

A general requirement of the management system according to chapter 8 of EN-ISO/IEC 17065/2012 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 of Regulation (EU) 2016/679 and thereafter at the request of the data protection supervisory authority at any time during an investigation in the form of data protection reviews pursuant to Article 58(1)(b) of Regulation (EU) 2016/679 or a review of the certifications issued in accordance with Article 42(7) of Regulation (EU) 2016/679 pursuant to Article 58(1)(c) of Regulation (EU) 2016/679.

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 Regulation (EU) 2016/679).

8.1 Options

The requirements of EN-ISO/IEC 17065/2012 shall apply.

8.2 General management system documentation

The requirements of EN-ISO/IEC 17065/2012 shall apply.

8.3 Control of documents

The requirements of EN-ISO/IEC 17065/2012 shall apply.

8.4 Control of records

The requirements of EN-ISO/IEC 17065/2012 shall apply.

8.5 Management review

The requirements of EN-ISO/IEC 17065/2012 shall apply.

8.6 Internal audits

The requirements of EN-ISO/IEC 17065/2012 shall apply.

8.7 Corrective actions

The requirements of EN-ISO/IEC 17065/2012 shall apply.

8.8 Preventive actions

The requirements of EN-ISO/IEC 17065/2012 shall apply.

CHAPTER IX: FURTHER ADDITIONAL REQUIREMENTS

Section 1: 9.1. Updating of evaluation methods

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

Section 2: 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 development listed in point 9.1.

Section 3: 9.3. Responsibilities and competencies

(1) 9.3.1 Communication between CB and its clients

Procedures shall be in place for implementing appropriate procedures and communication structures between the certification body and its client. 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 ANSPDCP with respect to
        i. feedback
        ii. decisions of ANSPDCP.

(2) 9.3.2 Documentation of evaluation activities

No additional requirements are laid down.

(3) 9.3.3 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 points 4.1.2.2 lit. c), 4.1.2.2 lit. j), 4.6 lit. d) and 7.13 of EN-ISO/IEC 17065/2012.

Relevant complaint and objections shall be shared with the RO SA.

(4) 9.3.4 Management of withdrawal

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

Published within the Official Gazette under number 689 from 12th of July 2021