Additional accreditation requirements for certification bodies with regard to ISO/IEC 17065/2012 and in compliance with Article 43 (1) letter b) of the General Data Protection Regulation

Hungary

Introduction

The Hungarian National Authority for Data Protection and Freedom of Information (Nemzeti Adatvédelmi és Információszabadság Hatóság, hereinafter referred to as NAIH) adopts the following document on the accreditation requirements for certification bodies with respect to ISO/IEC 17065/2012 and in accordance with Articles 43 (1) b) and 43 (3) of the General Data Protection Regulation[1] (hereinafter referred to as GDPR).

This document should be read in conjunction with ISO/IEC 17065/2012. Section numbers used here correspond to those used in ISO/IEC 17065/2012.

0 Prefix

The rules of the accreditation procedure of a certification body in Hungary are set out in Act CXXIV of 2015 on National Accreditation[2]. The accreditation of data protection certification bodies is performed by the Hungarian National Accreditation Authority (Nemzeti Akkreditáló Hatóság, hereinafter referred to as NAH).

According to Section 5 (1) l) of the abovementioned Act, application for accreditation and/or extension procedure shall be submitted by the natural person or the certification body (hereinafter: data protection certification body) according to Article 43 of the GDPR electronically to the NAH.

Section 5 (4) provides that accreditation can be requested by a data protection certification body which is in compliance with the organizational, personnel and operational requirements laid down in the GDPR.

Based on Section 6 (1) and (2a), the accreditation procedure consists of an assessment and decision-making phases. In the assessment phase of the accreditation procedure and extension of scope procedure of a data protection certification body, the NAIH shall be involved concerning compliance with the requirements laid down in the GDPR.

When performing a specialist authority procedure, the administrative deadline for the NAIH is fifty days.[3] An administrative service fee is payable for the accreditation procedure, the procedure for the extension of the scope of the accredited status, the surveillance procedure launched in response to an application and for the recognition of a foreign accredited status.

[1] 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
[2] https://nah.gov.hu/uploads/attachment/file/8145/2015._%C3%A9vi_CXXIV__en_2019.05.12.pdf
[3] Article 6 (5a) of Act CXXIV of 2015 on National Accreditation

The administrative service fee payable for the procedure performed as specialist authority by the NAIH shall be paid as part of, and together with the administrative service fee paid for the accreditation procedure, the procedure for the extension of the scope of the accredited status and the surveillance procedure launched in response to an application.[4]

More details on the accreditation procedure can be found in Act CXXIV of 2015 on National Accreditation and Act CL of 2016 on the Code of General Administrative Procedure[5].

The operational procedures in relation to accreditation of certification bodies are set out in a publicly available binding agreement between NAIH and NAH, which are made public on both organisations' website.

1 Scope

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

The scope of ISO/IEC 17065/2012 shall be applied in accordance with the GDPR. The European Data Protection Board's (hereinafter referred to as EDPB) guidelines on accreditation and certification[6] provide further information. The scope of a certification mechanism (for example, certification of cloud service processing operations) should be taken into account in the assessment by NAH and NAIH during the accreditation process, particularly with respect to criteria, expertise and evaluation methodology. The broad scope of 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 (1), GDPR certification is only applicable to the processing operations of controllers and processors.

2 Normative reference

GDPR has precedence over ISO/IEC 17065/2012. 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

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

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

[4] Articles 7 (1) and (2) of Act CXXIV of 2015 on National Accreditation
[5] http://njt.hu/translated/doc/J2016T0150P_20190710_FIN.pdf
[6] Guidelines 4/201 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation; and Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the General Data Protection Regulation

- Accreditation: third party attestation related to the activities of a certification body. This is the result of the assessment process for successful certification body (as part of the accreditation process).
- National accreditation body (NAB): the sole body in a Member State named in accordance with Regulation (EC) No 765/2008 of the European Parliament and Council that performs accreditation with authority derived from the State. In Hungary the NAB is the Hungarian National Accreditation Authority (Nemzeti Akkreditáló Hatóság, NAH).
- Accreditation body: body that performs accreditation. In this document this term designates the NAH.
- Certification body (CB): third party conformity assessment body operation certification schemes.
- Certification criteria: the criteria against which an organisation's processing operations are measured for a given certification scheme.
- Certification scheme: a certification system related to specified products, processes and services to which the same specified requirements, specific rules and procedures apply. It includes the certification criteria and assessment methodology.
- Certification mechanism: an approved certification scheme which is available to the applicant. It is a service provided by an accredited certification body based on approved criteria and assessment methodology. It is the system by which a controller or processor becomes certified.
- Target of Evaluation (ToE): the object of the 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 organization that has applied to have their processing operations certified.
- Client: the organization that has been certified (previously the applicant).

4 General requirements for accreditation

4.1. Legal and contractual matters

4.1.1. Legal responsibility

A certification body shall be able to demonstrate (at all times) to the NAH and NAIH 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 GDPR 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 provide evidence of compliance as required during the accreditation process. This shall include the certification body confirming to the accreditation body that they are not the subject of any NAIH investigation of any type.

4.1.2. Certification agreement (“CA”)

The certification body shall demonstrate in addition to the requirements of ISO/IEC 17065/2012 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 lit. a ISO/IEC 17065/2012 and the criteria approved by NAIH or the EDPB in accordance with Article 43 (2) (b) and Article 42 (5) GDPR;
2. require the applicant to allow full transparency to NAIH with respect to the certification procedure including contractually confidential matters related to data protection compliance pursuant to Articles 42 (7) and 58 (1) (c) GDPR;
3. do not reduce the responsibility of the applicant for compliance with the GDPR and is without prejudice to the tasks and powers of NAIH which is competent in line with Article 42 (5) 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) 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 lit. c No. 1 ISO/IEC 17065/2012 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;
7. allow the certification body to disclose all information necessary for granting certification pursuant to Articles 42(8) and 43(5);
8. include rules on the necessary precautions for the investigation of complaints within the meaning of 4.1.2.2 lit. c No. 2, 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;
9. in addition to the minimum requirements referred to in 4.1.2.2 ISO/IEC 17065/2012, if the consequences of withdrawal or suspension of accreditation for the certification body impact on the client, in that case the consequences for the customer shall all also be addressed;
10. require the applicant to inform the certification body in the event of significant changes in its actual or legal situation and in its products, processes and services concerned by the certification, as well as in the event of data protection infringements relevant to the ToE and established by NAIH or the competent judicial authority;
11. includes binding evaluation methods with respect to the ToE.

4.1.3. Use of data protection seals and marks

Certificates, seals and marks shall only be used in compliance with Article 42 and 43 of the GDPR and the guidelines on accreditation and certification.

4.2. Management of impartiality

The NAH shall ensure that in addition to the requirements set out in ISO/IEC 17065/2012, in particular 3.13 and 4.2, and the requirements of Regulation 765/2008/EC, in particular Article 17 (3), that the certification body:

1. complies with the additional requirements of NAIH (pursuant to Article 43 (1) (b)) as set out in this document;
    a. in line with Article 43 (2) (a) 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. has demonstrated that its tasks and obligations do not lead to a conflict of interest pursuant to Article 43 (2) (e) GDPR;
2. has no relevant connection with the applicant it assesses (e.g. the certification body shall not belong to the same company group nor shall it be controlled in any way by the customer it assesses).

4.3. Liability and financing

In addition to the requirement in 4.3.1 ISO/IEC 17065/2012, the certification body shall demonstrate to the NAH on a regular basis that it has appropriate measures (e.g. insurance or reserves) to cover its liabilities in the geographical regions in which it operates.

4.4. Non-discriminatory conditions

Requirements of ISO/IEC 17065/2012 shall apply.

4.5. Confidentiality

Requirements of ISO/IEC 17065/2012 shall apply.

4.6. Publicly available information

In addition to the requirements in 4.6 ISO/IEC 17065/2012, the certification body shall demonstrate to the NAH that:

1. 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, and the respective period of validity;
2. information about complaints handling procedures and appeals are made public pursuant to Article 43 (2) (d) GDPR.

5 Structural requirements, Article 43 (4) [“proper” assessment]

5.1. Organisational structure and top management

Requirements of ISO/IEC 17065/2012 shall apply.

5.2. Mechanisms for safeguarding impartiality

Requirements of ISO/IEC 17065/2012 shall apply.

6 Resource requirements

6.1. Certification body personnel

The accreditation body shall in addition to the requirement in section 6 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) GDPR;
2. has independence and ongoing expertise with regard to the object of certification pursuant to Article 43 (2) (a) GDPR and does not have a conflict of interest pursuant to Article 43 (2) (e) GDPR;
3. undertakes to respect the criteria referred to in Article 42 (5) GDPR pursuant to Article 43 (2) (b) 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 additional requirements 6.1.1, 6.1.4, and 6.1.5, specifically

For personnel with technical expertise:

- Have obtained a qualification in a relevant area of technical expertise to at least EQF[7] level 6 or a recognised protected title in the relevant regulated profession.
- *Personnel responsible for certification decisions* require significant professional experience in identifying and implementing data protection measures.
- *Personnel responsible for evaluations* require professional experience in technical data protection and knowledge and documented experience in comparable procedure (e.g. certifications/audits), and registered as applicable.

For personnel with legal expertise:

- Legal studies at an EU or state-recognised university for at least eight semesters including the academic degree Master or equivalent.
- *Personnel responsible for certification decisions* shall demonstrate at least five years of professional – and relevant for the to be performed tasks - experience in data protection law.
- *Personnel responsible for evaluations* shall demonstrate at least three years of professional experience in data protection law and knowledge and experience in comparable procedures (e.g. certifications/audits).

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

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

Proof of knowledge can be demonstrated by documents relating to appropriate professional qualifications or courses (e.g. training certificates) attesting to the qualifications or competencies required.

6.2. Resources for evaluation

Requirements of ISO/IEC 17065/2012 shall apply.

7 Process requirements[8]

7.1. General

In addition to the requirements of ISO/IEC 17065/2012, the NAIH shall ensure the following:

1. the certification bodies comply with these additional requirements (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) (b) GDPR;
2. the relevant competent supervisory authorities are notified before a certification body starts operating an approved European Data Protection Seal in a new Member State from a satellite office.

7.2. Application

In addition to the requirements in 7.2 of ISO/IEC 17065/2012, the certification body shall require that:

1. 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;
2. the application shall specify whether processors are used, and when processor is the applicant, that their responsibilities and tasks shall be described, and the application shall contain the relevant controller/processor contract(s);
3. specifies whether joint controllers are involved in the processing, and where the joint controller is the applicant, their responsibilities and tasks shall be described, and the application shall contain the agreed arrangement;
4. discloses any current or recent NAIH investigation or procedure of any kind to which the applicant is subject, and which is relevant to the scope of certification and the ToE.

7.3. Application Review

In addition to item 7.3 of ISO/IEC 17065/2012, the assessment of competence and capability referred to in 7.3.1. (e) of ISO 17065/2012 shall take into account, as per section 6 above, both technical and legal expertise in data protection to an appropriate extent.

[8] Article 43 (2) (c) and (d) GDPR

The application review shall take into account the data protection compliance checks referred to in point 7.2.4. of this document. The certification body is required to satisfy themselves that the applicant is a fit candidate for data protection certification.

7.4. Evaluation

In addition to item 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 of GDPR, and with regard to the definition of technical and organisational measures pursuant to Articles 24, 25 and 32 of GDPR, insofar as the aforementioned Articles apply to the target of evaluation, 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 criteria are met; and
4. documentation of methods and findings.

The certification body shall be required to ensure that these evaluation methods are standardized and 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/IEC 17065/2012, it shall be allowed that the evaluation is carried out by external experts who have been recognized by the certification body, using the same personnel requirements as in Section 6 of this document. The certification body will retain the responsibility for the decision-making even when it uses external experts.

In addition to item 7.4.5 of ISO/IEC 17065/2012, it shall be required that data protection certification in accordance with Articles 42 and 43 of GDPR, which already covers part of the target of evaluation, 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 previous certification activity 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/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 item 7.4.6 informs the applicant about nonconformities with the certification mechanism. In this context, at least the nature and timing of such information shall be defined.

In addition to item 7.4.9 of ISO/IEC 17065/2012, it shall be required that documentation be made fully accessible to NAIH upon request.

7.5. Review

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

7.6. Certification decision

In addition to point 7.6.1 of 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 is ensured.

In order to assure transparency, in addition to the requirements of ISO/IEC 17065/2012, 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 NAIH. The executive summary will clearly describe how the criteria are met thus providing the reasons for granting or maintaining the certification. Even if the NAIH decides, on the basis of the information submitted, to start an investigation, it will not suspend the certification process.

In addition to the check carried out at the application stage, prior to issuing certification, the certification body shall be required to confirm with the applicant that they are not the subject of any NAIH investigation or procedure of any kind related to the target of evaluation or the scope of the certification, which might prevent certification being issued.

7.7. Certification documentation

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

In addition to item 7.7.1.f of ISO/IEC 17065/2012, 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 NAIH with a copy of the certification documentation referred to in 7.7.1. of ISO/IEC 17065/2012.

7.8. Directory of certified products

In addition to item 7.8 of ISO/IEC 17065/2012, the certification body shall 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:

- the scope of the certification and a meaningful description of the target of evaluation (ToE),
- the respective certification criteria (including version or functional status),
- the evaluation methods and tests conducted and

- the result(s).

In addition to item 7.8 of ISO/IEC 17065/2012 and pursuant to Article 43 (5) of GDPR, the certification body shall inform the competent supervisory authorities 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/IEC 17065/2012, 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. When determining the periodicity of the surveillance, the risk associated with the processing should be the primary factor to consider, but in any case, the surveillance should take place *at least* every two years.

7.10. Changes affecting certification

In addition to points 7.10.1 and 7.10.2 of ISO/IEC 17065/2012, changes affecting certification to be considered by the certification body shall include:

- any high-risk personal data breach occurred, or infringements of the GDPR established by NAIH or the competent judicial authority, that is related to the target of evaluation, reported by the client or NAIH;
- amendments to data protection legislation or the state of the art,
- the adoption of delegated acts of the European Commission in accordance with Articles 43 (8) and 43 (9) of GDPR,
- applicable documents adopted by the EDPB, and
- court decisions related to data protection.

The change procedures to be agreed here could include such things as: transition periods, approvals process with NAIH, 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 7.11.1 of ISO/IEC 17065/2012, the certification body shall be required to inform the NAIH and the NAH immediately in writing about measures taken, and about 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 NAIH to withdraw or not to issue certification to an applicant if the requirements for certification are not or no longer met.

7.12. Records

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

7.13. Complaints and appeals[9]

In addition to item 7.13.1 of ISO/IEC 17065/2012, the certification body shall be required to define,

- who can file complaints or objections,
- who processes them on the part of the certification body,
- which verifications take place in this context; and
- the possibilities for consultation of interested parties.

In addition to item 7.13.2 of ISO/IEC 17065/2012, the certification body shall be required to define,

- how and to whom such confirmation must be given,
- the time limits for this; and
- which processes are to be initiated afterwards.

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

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

In addition to item 7.13.1 of ISO/IEC 17065/2012, the certification body must define how separation between certification activities and the handling of appeals and complaints is ensured.

8 Management system requirements

A general requirement of the management system according to chapter 8 of ISO/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 in the accreditation procedure pursuant to Article 58 GDPR and thereafter at the request of the NAIH at any time during an investigation

[9] Article 43 (2) d) GDPR

in the form of data protection reviews 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) of 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[10].

For the purpose of transparency, the certification body shall:

- keep track of the principles underlying the conformity assessment (e.g. reference technical standards, laws and regulations, etc.);
- document the specific methodologies applied in defining audit procedures for the conformity assessment;
- document inspection and audit activities and the improvements made to the existing procedures including the reasons and the time-schedule for such improvements;
- document and monitor compliance with impartiality requirements;
- give reasons for any changes to the records and process transparency requirements with regard to individual certification schemes, the arrangements for assessing conformity with such schemes, and the minimum requirements set forth in certification agreements with clients.

8.1. General management system requirements

Requirements of ISO/IEC 17065/2012 shall apply.

8.2. Management system documentation

Requirements of ISO/IEC 17065/2012 shall apply.

8.3. Control of documents

Requirements of ISO/IEC 17065/2012 shall apply.

8.4. Control of records

Requirements of ISO/IEC 17065/2012 shall apply.

8.5. Management Review

Requirements of ISO/IEC 17065/2012 shall apply.

8.6. Internal audits

Requirements of ISO/IEC 17065/2012 shall apply.

8.7. Corrective actions

Requirements of ISO/IEC 17065/2012 shall apply.

8.8. Preventive actions

[10] Recital 100 of GDPR

Requirements of ISO/IEC 17065/2012 shall apply.

9 Further additional requirements

9.1. Updating of evaluation methods

The certification body shall establish procedures to guide the updating of evaluation methods for application in the context of the evaluation under point 7.4. 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.

9.3. Responsibilities and competencies

9.3.1. Communication between CB and its clients and applicants

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

1. maintaining documentation of tasks and responsibilities by the accredited certification body, for the purpose of
    - information requests, or
    - to enable contact in the event of a complaint about a certification;
2. maintaining an application process for the purpose of
    - information on the status and outcome of an application;
    - evaluations by the NAIH with respect to

        feedback;

        decisions by the NAIH.

9.3.2. Documentation of evaluation activities

No additional requirements are laid down.

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 ISO/IEC 17065/2012.

Relevant complaint and objections shall be shared with the NAIH.

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.