AUTORITEIT
PERSOONSGEGEVENS

NL additional accreditation requirements for certification bodies

The Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*, hereinafter: AP) has on 8 June 2021 adopted the following decision on the additional accreditation requirements for certification bodies with respect to ISO/IEC 17065:2012 (hereinafter ISO 17065) and in accordance with Articles 43(1)(b) and 43(3) of the GDPR:

The points below (aside from section 9) refer to ISO 17065 section headings and set out the additional requirements for the relevant ISO 17065 section numbers.

0 Prefix

The roles and responsibilities of the AP and the *Raad voor Accreditatie* (hereinafter: RvA) as the Dutch National Accreditation Body (NAB) in relation to accreditation for GDPR certification schemes are set out in the Dutch GDPR Implementation Act (*Uitvoeringswet Algemene Verordening Gegevensbescherming*, hereinafter: UAVG) and in a ministerial regulation (*Regeling van de Minister voor Rechtsbescherming van 16 mei 2018 tot aanwijzing van de Raad voor Accreditatie als accrediterende instantie als bedoeld in artikel 43, eerste lid, van de Algemene verordening gegevensbescherming*).[1] The operational procedures in relation to accreditation for GDPR certification schemes are set out in a publicly available binding agreement between the AP and the RvA.[2]

1 Scope

This document contains additional requirements to ISO 17065 for assessing the competence, consistent operation and impartiality of GDPR certification bodies.

The scope of ISO 17065 shall be applied in accordance with the GDPR. The EDPB guidelines on accreditation and certification provide further information. The broad scope of ISO 17065 covering products, processes and services does not lower or override the requirements of the GDPR. Therefore, certification must be in respect of personal data processing operations. And whilst a governance system, for example a privacy information management system, can form part of a certification mechanism, it cannot be the only element.

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

[1] Staatscourant 2018, 28116.
[2] Staatscourant 2020, 11507.

Finally, pursuant to Article 42(1) of the GDPR, GDPR certification can only be awarded in relation to controller and processor's processing operations.

2 Normative reference

The 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[3] and certification[4] shall apply and have precedence over ISO definitions. For ease of reference the main definitions used in this document are listed below.

- General Data Protection Regulation (GDPR): Regulation 2016/679/EC.
- UAVG: *Uitvoeringswet Algemene Verordening Gegevensbescherming*, the Dutch GDPR Implementation Act.
- ISO 17065: ISO/IEC 17065:2012.
- Certification: the assessment and impartial, third-party attestation that the fulfilment of certification criteria has been demonstrated in respect of a controller or processor's processing operations.
- Accreditation: 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 the Council that performs accreditation with authority derived from the State. In the Netherlands the NAB is the *Raad voor Accreditatie* (RvA).
- Accreditation body: body that performs accreditation. In this document this term is taken to mean RvA.
- Certification body: third party conformity assessment body operating certification schemes.
- Certification criteria: the criteria against which an organisation's processing operations are measured for a given certification scheme.
- Certification scheme: a certification system related to specified products, processes and services to which the same specified requirements, specific rules and procedures apply. It includes the certification criteria and assessment methodology.
- Certification mechanism: an approved certification scheme which is available to the applicant. It is a service provided by an accredited certification body based on approved criteria and assessment methodology. It is the system by which a controller or processor becomes certified.
- Target of Evaluation (ToE): the object of certification. In the case of GDPR certification this will be the relevant processing operations that the controller or processor is applying to have evaluated and certified.
- Applicant: the organisation that has applied to have their processing operations certified.
- Client: the organisation that has been certified (previously the applicant).

[3] Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the General Data Protection Regulation.
[4] Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation.

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 RvA that they have up to date procedures that demonstrate compliance with the legal responsibilities set out in the terms of accreditation, including the additional requirements in respect of the application of the GDPR.

The certification body shall be able to demonstrate that its procedures and measures specifically for controlling and handling of applicant and client organisation's personal data as part of the certification process are compliant with the GDPR and the UAVG. As such it shall be able to provide evidence of compliance as required during the accreditation process.

The certification body shall provide evidence of compliance as required during the accreditation process.

This shall include the certification body confirming to the RvA that they are not the subject of any AP investigation or regulatory action which may mean they do not meet this requirement and therefore might prevent their accreditation.

4.1.2 Certification agreement

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

1 require the applicant to always comply with both the general certification requirements within the meaning of 4.1.2.2(a) of ISO 17065 and the criteria approved by the AP or the EDPB in accordance with Article 43(2)(b) and Article 42(5) of the GDPR;
2 require the applicant to allow full transparency to the AP with respect to the certification procedure, including any confidential materials, whether contractual or otherwise, related to data protection compliance pursuant to Articles 42(7) and 58(1)(c) of the GDPR;
3 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;
4 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 mechanism or other regulations must be observed and adhered to;
5 allow the certification body to disclose to the AP the reasons for granting or withdrawing the certification, pursuant to Article 43(5) of the GDPR, and the information that the AP will need to provide to the EDPB in order to enable the EDPB to include the certification mechanism in a publicly available register pursuant to Article 42(8) of the GDPR;
6 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);

7 require the applicant to inform the certification body in the event of infringements of GDPR or the UAVG that are established by the AP and/or the judicial authorities and that may affect its certification, as soon as they become aware of such an infringement.
8 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 in line with Article 42(7) of the GDPR and section 7.9 of these requirements;
9 in addition to the minimum requirements referred to in 4.1.2.2 of ISO 17065, if the consequences of withdrawal or suspension of the accreditation of the certification body have impact on the client, any consequences for the customer are also addressed.
10 do not reduce the responsibility of the applicant or the client to comply, as applicable, with the GDPR and is without prejudice to the tasks and powers of the competent supervisory authorities in line with Article 42(5) of the GDPR;
11 includes binding evaluation methods with respect to the Target of Evaluation (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

In addition to the requirements of ISO 17065, in particular 3.13 and 4.2, the certification body shall demonstrate to the RvA:

1 that the certification body complies with the additional requirements of the AP (pursuant to Article 43(1)(b) of the GDPR) as set out in this document;
2 in line with Article 43(2)(a) of the GDPR the certification 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;
3 that the tasks and obligations of the certification body do not lead to a conflict of interest pursuant to Article 43(2)(e) of the GDPR;
4 that the certification body has no relevant connection with the applicant it assesses.

4.3 Liability and financing

In addition to the requirement in 4.3.1 of ISO 17065, the certification body shall demonstrate to the RvA on a regular basis (i.e. once a year) that it has appropriate measures (e.g. insurance and/or reserves) to cover its liabilities in the geographical regions in which it operates. Furthermore, the certification body shall demonstrate its financial stability and independence. The decision with respect to the selection and designation of the supporting documents lies within the discretion of the RvA.

4.4 Non-discriminatory conditions

Requirements in 4.4 of ISO 17065 shall apply.

4.5 Confidentiality

Requirements in 4.5 of ISO 17065 shall apply.

4.6 Publicly available information

In addition to the requirements in 4.6 of ISO 17065, the certification body shall demonstrate to the RvA that:

1 all versions (current and previous) of the approved criteria under Article 42(5) of the GDPR are published and easily publicly available as well as a high-level and meaningful explanation about the 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) of the GDPR.

5 Structural requirements[5]

5.1 Organisational structure and top management

Requirements in 5.1 of ISO 17065 shall apply.

5.2 Mechanisms for safeguarding impartiality

Requirements in 5.2 of ISO 17065 shall apply.

6 Resource requirements

6.1 Certification body personnel

In addition to the requirement in section 6 of ISO 17065, the certification body shall demonstrate to the RvA 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 object of certification pursuant to Article 43(2)(a) of the GDPR and does 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 demonstrable, relevant and appropriate knowledge about and experience in applying data protection legislation, with evaluators having a more specialist expertise and professional experience in technical procedures (e.g. audits and certifications), while decision-makers have a more general and comprehensive expertise and professional experience in data protection;
5 has demonstrable, relevant and appropriate knowledge about and experience in technical and organisational data protection measures as relevant;

[5] Article 43(4) of the GDPR ["proper" assessment].

6 is able to demonstrate experience in the fields mentioned in these additional requirements, specifically:

For personnel with technical expertise:
- Have obtained a qualification in a relevant area of technical expertise to at least EQF[6] level 6 or a recognised protected title (e.g. Dipl. Ing.) in the relevant regulated profession, or have significant relevant professional experience in that field.
- 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 experience in comparable procedure (e.g. certifications/audits), and registered as applicable.
- Personnel shall demonstrate they maintain domain specific knowledge in technical and audit skills through continuous professional development.

For personnel with legal expertise:
- Legal studies at an EU or state-recognised university for at least eight semesters including the academic degree Master (LL.M.) or equivalent, or significant professional experience.
- Personnel responsible for certification decisions shall demonstrate significant professional experience in data protection law and be registered as applicable.
- Personnel responsible for evaluations shall demonstrate at least two years of professional experience in data protection law and knowledge and experience in comparable procedures (e.g. certifications/audits), and be registered as applicable.
- Personnel shall demonstrate they maintain domain specific knowledge in legal and audit skills through continuous professional development.

6.2 Resources for evaluation

Requirements of 6.2 of ISO 17065 shall apply.

7 Process requirements[7]

7.1 General

In addition to the requirement in 7.1 of ISO 17065, the RvA shall ensure the following:
1 that certification bodies meet these additional requirements (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)(e) of the GDPR;
2 that the relevant competent supervisory authority is notified before a certification body starts operating an approved European Data Protection Seal in a new Member State from a satellite office.

[6] See qualification framework comparison tool at https://ec.europa.eu/ploteus/en/compare?
[7] Article 43(2)(c),(d) of the GDPR.

7.2 Application

In addition to item 7.2 of ISO 17065, the certification body shall require that the application:

1 contains a detailed description of the object of certification (Target of Evaluation, ToE). This also includes interfaces and transfers to other systems and organisations, protocols and other assurances;
2 specifies whether processors are used, and when processors are the applicant, their responsibilities and tasks shall be described, and the application shall contain the relevant controller/processor contract(s);
3 specifies whether joint controllers are involved in the processing, and where the joint controller is the applicant, their responsibilities and tasks shall be described, and the application shall contain the agreed arrangement; and
4 discloses any current or recent AP investigation or regulatory action that is related to the scope of certification and the target of evaluation to which the applicant is subject.

7.3 Application review

In addition to item 7.3 of ISO 17065:

- the assessment in 7.3(e) of ISO 17065 of whether there is sufficient expertise shall take into account both technical and legal expertise in data protection to an appropriate extent;
- the application review shall take into account the data protection compliance checks referred to in 7.2(4) of this document, and the certification body shall satisfy themselves that the applicant is a fit candidate for data protection certification.

7.4 Evaluation

In addition to item 7.4 of ISO 17065, the certification scheme shall describe sufficient evaluation methods for assessing the compliance of the processing operation(s) with the certification criteria, including such areas as:

1 a method for assessing the necessity and proportionality of processing operations in relation to their purpose and the data subjects concerned;
2 a method for evaluating the coverage, composition and assessment of all risks considered by controller and processor with regard to the legal consequences pursuant to Articles 30, 32 and 35 and 36 of the GDPR, and with regard to the definition of technical and organisational measures pursuant to Articles 24, 25 and 32 of the GDPR, insofar as the aforementioned Articles apply to the object of certification, and
3 a method for assessing the remedies, including guarantees, safeguards and procedures to ensure the protection of personal data in the context of the processing to be attributed to the object of certification and to demonstrate that the legal requirements as set out in the adopted criteria are met; and
4 documentation of methods and findings.

The certification body shall be required to ensure that these evaluation methods are standardised and applied consistently. This means that comparable evaluation methods are used for comparable ToEs. Any deviation from this procedure shall be justified by the certification body.

In addition to item 7.4.2 of ISO 17065 the evaluation may be carried out by sub-contractors who have been recognised by the certification body, using the same personnel requirements in section 6.

In addition to item 7.4.5 of ISO 17065, it shall be provided that existing certification, which relates to the same object of certification, may be taken into account as part of a new evaluation. However, the certificate alone will not be sufficient evidence and the certification body shall be obliged to check the compliance with the criteria in respect of the object of certification. The complete evaluation report and other relevant information enabling an evaluation of the existing certification and its results shall be considered in order to make an informed decision.

In cases where existing certification is taken into account as part of a new evaluation, the scope of said certification should also be assessed in detail in respect of its compliance with the relevant certification criteria.

In addition to item 7.4.6 of ISO 17065, it shall be required that the certification body shall set out in detail in its certification scheme how the information required in item 7.4.6 informs the applicant about nonconformities with the scheme. This will include as a minimum the nature and timing of such information.

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

7.5 Review

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

7.6 Certification decision

In addition to item 7.6.1 of ISO 17065, the certification body shall be required to set out in detail in its procedures how its independence and responsibilities with regard to individual certification decisions are ensured.

In addition to item 7.6 of ISO 17065, immediately prior to issuing or renewing certification, the certification body shall be required to inform the AP by submitting the draft approval, including the executive summary of the evaluation report to the AP. The executive summary will clearly describe how the criteria are met thus providing the reasons for granting or maintaining the certification.

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 AP investigation or regulatory action which might prevent certification being issued.

7.7 Certification documentation

In addition to item 7.7.1(e) of ISO 17065 and in accordance with Article 42(7) of the GDPR, it shall be required that the period of validity of certifications shall not exceed three years.

In addition to item 7.7.1(e) of ISO 17065, it shall be required that the period of the intended monitoring within the meaning of section 7.9 of this document is documented.

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

On issuing the certificate, the certification body shall be required to provide the AP with a copy of the certification documentation referred to in 7.7.1 of ISO 17065.

7.8 Directory of certified products

In addition to 7.8 of ISO 17065, the certification body shall make publicly accessible a record of the certifications issued and on which basis, including information about the certification mechanism, and how long the certifications are valid for.

The certification body will provide to the public an executive summary of the evaluation report. The aim of this executive summary is to help with transparency around what has been certified and how it was assessed. It will explain such things as:

a) the scope of the certification and a meaningful description of the object of certification (ToE),
b) the respective certification criteria (including version or functional status),
c) the evaluation methods and tests conducted and
d) the result(s).

7.9 Surveillance

In addition to items 7.9.1, 7.9.2 and 7.9.3 of ISO 17065, and according to Article 43(2)(c) of the GDPR requires regular monitoring measures to maintain certification during the monitoring period. Such measures should be risk based and proportionate and the maximum period between surveillance activities should not exceed 12 months.

7.10 Changes affecting certification

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

- any personal data breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons, or infringement of the GDPR or the UAVG established by the AP and/or the judicial authorities that is related to the object of certification, reported by the client or the AP;
- 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;
- documents adopted by the European Data Protection Board; and
- court decisions related to data protection;
- changes in the state of the art related to data protection or to the object of certification.

The change procedures to be implemented by the certification body shall include such things as: transition periods, approvals process with the AP, reassessment of the relevant object of certification 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 AP and the RvA immediately in writing about measures taken and about continuation, restrictions, suspension and withdrawal of certification.

Where the AP determines requirements for the certification are not or are no longer met, in line with Article 58(2)(h) of the GDPR, the certification body shall accept decisions or orders to withdraw or not issue certification.

7.12 Records

In addition to 7.12 of ISO 17065, the certification body is required to keep all documentation complete, comprehensible, up-to-date and fit to audit.

7.13 Complaints and appeals

In addition to item 7.13.1 of ISO 17065, the certification body shall define,
a) who can file complaints or objections,
b) who processes them on the part of the certification body,
c) which verifications take place in this context; and
d) the possibilities for consultation of interested parties.

In addition to item 7.13.2 of ISO 17065, the certification body shall define,
a) how and to whom such confirmation must be given,
b) the time limits for this; and
c) which processes are to be initiated afterwards.

Certification bodies shall 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/or the outcome of the complaint without undue delay, and in any event within one month of receipt of the complaint. This period may be extended where necessary. In this case, the certification body shall inform the complainant within one month of receipt of the request of when the outcome can be expected.

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

8 Management system requirements

In addition to chapter 8 of ISO 17065, 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 of the GDPR and thereafter at the request of the AP at any time during an investigation in the form of data protection audits 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.

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

A complaints handling process with the necessary levels of independence shall be established by the certification body as an integral part of the management system, which shall in particular implement the requirements of points 4.1.2.2(c), 4.1.2.2(j), 4.6(d) and 7.13 of ISO 17065.

8.1 General management system requirements

Requirements of 8.1 Options of ISO 17065 shall apply.

8.2 Management system documentation

Requirements of 8.2 of ISO 17065 shall apply.

8.3 Control of Documents

Requirements of 8.3 of ISO 17065 shall apply.

8.4 Control of records

Requirements 8.4 of ISO 17065 shall apply.

8.5 Management review

Requirements of 8.5 of ISO 17065 shall apply.

8.6 Internal audits

Requirements of 8.6 of ISO 17065 shall apply.

8.7 Corrective actions

Requirements of 8.7 of ISO 17065 shall apply.

8.8 Preventive actions

Requirements of 8.8 of ISO 17065 shall apply.

9 Further additional requirements

9.1 Updating of evaluation methods

The certification body shall establish procedures to guide the updating of evaluation methods for application in the context of the evaluation under point 7.4 of ISO 17065 and this document. The update must take place in the course of changes in the legal framework, the relevant risk(s), the state of the art and the implementation costs of technical and organisational measures.

9.2 Maintaining expertise

Certification bodies shall establish procedures to ensure the training of their employees with a view to updating their skills, taking into account the developments listed in point 9.1 of this document.

9.3 Responsibilities and competencies

9.3.1 Communication between the certification body and its clients and applicants

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

1 Maintaining documentation of tasks and responsibilities by the accredited certification body, for the purpose of
   - responding to 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 AP with respect to
     - feedback;
     - decisions by the AP.

9.3.2 Documentation of evaluation activities

No additional requirements apply.

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(c), 4.1.2.2(j), 4.6(d) and 7.13 of ISO 17065.

Relevant complaint and objections should be shared with the AP.

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 notification of clients.