UK additional accreditation requirements for certification bodies (A.43(1)(b))

This document provides the Information Commissioner's additional accreditation requirements with respect to ISO/IEC 17065/2012 (hereinafter ISO 17065) and in accordance with Articles 43(1)(b) and 43(3) of the UK 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 Terms of cooperation between the Information Commissioner (ICO) and UK Accreditation Service (UKAS) as the UK's National Accreditation Body (NAB) are set out in a binding agreement. The binding agreement sets out roles and responsibilities and operational procedures in relation to accreditation for UK GDPR certification schemes.

1 Scope

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

The scope of ISO 17065 shall be applied in accordance with the UK GDPR. The broad scope of ISO 17065 covering products, processes and services does not lower or override the requirements of the UK 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 accreditation body during the accreditation process, particularly with respect to criteria, expertise and evaluation methodology.

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

2 Normative reference

The UK 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 UK GDPR.

3 Terms and definitions

EDPB guidelines are no longer directly relevant to the UK regime and are not binding under the UK regime. However, they may still provide helpful guidance on certain issues.

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.

UK GDPR: United Kingdom General Data Protection Regulation

DPA18: UK Data Protection Act 2018

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 that performs accreditation in the UK. The United Kingdom Accreditation Service (UKAS) is appointed as the NAB in the Accreditation Regulations 2009 - Statutory Instrument No.3155 to operate accreditation in accordance with the Regulation (EC) No.765/2008, as it has effect in the UK as a public authority activity.

Accreditation body: body that performs accreditation. In this document this term is taken to mean UKAS.

Certification body (CB): 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 UK 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).

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 UKAS 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 UK 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 UK GDPR and the UK Data Protection Act 2018 (DPA18). As such it shall be able to provide evidence of compliance as required during the accreditation process.

To this end, the certification body shall be required to confirm to the accreditation body that they are not the subject of any ICO investigation or regulatory action which may mean they do not meet this requirement and therefore might prevent their accreditation and to inform the accreditation body immediately of relevant infringements of UK GDPR or the DPA18 that may affect its accreditation. UKAS will verify this information with the ICO before proceeding with the accreditation process.

4.1.2 Certification agreement

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

1. require the client to always comply with both the general certification requirements within the meaning of 4.1.2.2(a) ISO 17065 and the criteria approved by the Commissioner in accordance with Article 43(2)(b) and Article 42(5);
2. require the client to allow full transparency to the ICO 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);
3. require the client 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);

4. require the client 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 ICO all information necessary for providing them with the reasons for granting the certification and to facilitate the ICO's publicly available register of UK GDPR approved certification mechanisms pursuant to Articles 43(5) and 42(8) respectively;
6. require the client to make its rules and procedures for complaint management (4.1.2.2(c)(2), and, (j)), transparent and easily accessible.
7. require the client to inform the certification body in the event of relevant infringements of UK GDPR or the DPA18 that may affect its certification, as soon as they become aware of such an infringement.
8. where the consequences of withdrawal or suspension of accreditation for the certification body impact on the client, the agreement shall also explain how any consequences for the customer (data subjects) will be addressed.
9. with respect to 4.1.2.2(c)(1) set out the rules of validity, renewal, and withdrawal pursuant to Articles 42(7) and 43(4) including rules setting appropriate intervals for re-evaluation or review in line with Article 42(7) and section 7.9 of these requirements;
10. do not reduce the responsibility of the client for compliance with UK GDPR and is without prejudice to the tasks and powers of the Commissioner;
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 and the guidelines on accreditation and certification.

4.2 Management of impartiality

Requirements of ISO 17065 shall apply.

4.3 Liability and financing

In addition to the requirements of ISO 17065, the accreditation body shall ensure that the certification body has appropriate measures (eg insurance and/or reserves) to cover its liabilities in the geographical regions in which it operates.

4.4 Non-discriminatory conditions

Requirements of ISO 17065 shall apply.

4.5 Confidentiality

Requirements of ISO 17065 shall apply.

4.6 Publicly available information

In addition to the requirements of ISO 17065, the accreditation body shall require from the certification body that:

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

5 Structural requirements [and Article 43(4) ["proper" assessment]

5.1 Organisational structure and top management

In addition to the requirements in 5.1.3 of ISO 17065, the accreditation body shall require the certification body to appoint a person with the relevant seniority with responsibility for overseeing data protection compliance and information governance.

5.2 Mechanisms for safeguarding impartiality

Requirements of ISO 17065 shall apply.

6 Resource requirements

6.1 Certification body personnel

In addition to the requirements of ISO 17065, the accreditation body shall ensure that certification body personnel undertaking certification conformity tasks:

1. have demonstrated appropriate expertise (knowledge and experience) with regard to data protection pursuant to Article 43(1);
2. have relevant and appropriate knowledge about and experience in applying data protection legislation including appropriate technical and organisational measures as relevant;
3. have independence and ongoing expertise with regard to the object of certification pursuant to Article 43(2)(a) and do not have a conflict of interest pursuant to Article 43(2)(e);
4. undertake to respect the criteria referred to in Article 42(5) pursuant to Article 43(2)(b);
5. demonstrate that they maintain relevant, specific knowledge in technical and audit skills through continuous professional development; and
6. is able to demonstrate experience in the fields mentioned in the additional requirements 6.1.1, 6.1.2, **and specifically**:
   - *Personnel providing technical expertise* must have obtained a qualification in a relevant area of technical expertise to at least EQF[1] level 6 [2] or have significant relevant professional experience in that field.

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

- *Personnel providing legal expertise* must have obtained a degree level (or equivalent) qualification in law and have significant professional experience in data protection law.

- *Personnel responsible for evaluations* must demonstrate relevant and recent professional experience and knowledge in technical data protection, and experience in comparable procedures (e.g. certifications/audits) and appropriate professional qualifications where relevant.

- *Personnel responsible for certification decisions* must have significant professional experience in identifying and implementing data protection measures, or access to someone with that expertise, and an appropriate professional/degree level qualification.

The certification body must be able to define and explain to the accreditation body which professional experience requirements are appropriate to the scope of the certification scheme and the target of evaluation in question.

6.2 Resources for evaluation

Requirements of ISO 17065 shall apply.

7 Process requirements, Article 43(2)(c), (d)

7.1 General

In addition to the requirements of ISO 17065, the accreditation body shall ensure the following:

1. that certification bodies meet these additional requirements (pursuant to Article 43(1)(b)) in order that tasks and obligations do not lead to a conflict of interests pursuant to Article 43(2)(e);
2. that certification bodies have procedures in place to notify the ICO immediately prior to issuing/renewing/withdrawing certifications and provide the reasons for taking such actions. This includes providing the ICO a copy of the executive summary of the evaluation report referenced in section 7.8 of this document.
3. that the certification body is required to carry out an investigation where the client or ICO notifies them of any significant and relevant investigation or regulatory action by the ICO in relation to the client that brings into question their data protection compliance. The certification body will undertake an investigation and provide the ICO with a report, advising of the outcome and whether the client still conforms to the certification criteria. This investigation will be related to the scope of the certification and the target of evaluation.

7.2 Application

In addition to the requirements 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 ICO investigation or regulatory action to which the applicant is subject.

The certification body shall be required to inform the ICO about all applications received at the application stage.

7.3 Application Review

In addition to the requirements of ISO 17065, the accreditation body shall require that the assessment in 7.3.1(e) takes 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. The certification body will be required to satisfy themselves that the applicant is a fit candidate for data protection certification.

7.4 Evaluation

In addition to the requirements 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 , and with regard to the definition of technical and organisational measures pursuant to Articles 24, 25 and 32 , 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.

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 need to 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 ICO upon request.

7.5 Review

Requirements of ISO 17065 shall apply.

7.6 Certification decision

In addition to the requirements of ISO 17065, immediately prior to issuing or renewing certification, the certification body shall be required to submit the draft approval, including the executive summary of the evaluation report to the ICO. 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 ICO investigation or regulatory action which might prevent certification being issued.

The ICO will confirm where appropriate that this is the case prior to the certification body issuing or renewing certification. If it is discovered that the applicant has not disclosed such action to the certification body, this may result in the certification not being issued.

7.7 Certification documentation

In addition to item 7.7.1(e) of ISO 17065 and in accordance with Article 42(7) , 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 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 ICO 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 the requirements 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, how long the certifications are valid for and under which framework and conditions.

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 points 7.9.1, 7.9.2 and 7.9.3 of ISO 17065, and according to Article 43(2)(c) 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 points 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 or infringement of UK GDPR or the DPA18 reported by the client or the ICO;
- amendments to data protection legislation;
- decisions, opinions, or guidanceissued by the ICO; and
- court decisions related to data protection.

The change procedures to be implemented by the certification body shall include such things as: transition periods, approvals process with the ICO, 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 point 7.11.1 of ISO 17065, and as detailed in section 7.1(2) of this document, the certification body should be required to inform the ICO immediately in writing about measures taken and about continuation, restrictions, suspension and withdrawal of certification.

Furthermore, in cases where the certification body determines non-compliance with the scheme it must define in its requirements what measures are to take place, and which cases (of non-compliance) constitute measures in the first place.

Where the ICO determines requirements for the certification are not or are no longer met, the ICO may order the certification body to withdraw or not issue certification in line with Art 58(2)h.

7.12 Records

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

7.13 Complaints and appeals, Article 43(2)(d)

In addition to point 7.13.1 of ISO 17065, the certification body should be required to define,

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

In addition to point 7.13.2 of ISO 17065, the certification body should 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.

Certification bodies should 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 point 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 the requirements of ISO 17065, management principles and their documented implementation must be transparent and be disclosed by the accredited certification body at the request of the ICO at any time during an investigation in the form of data protection audits pursuant to Art. 58(1)(b) or a review of the certifications issued in accordance with Article 42(7) pursuant to Article 58(1)(c).

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

Requirements of ISO 17065 shall apply.

8.2 Management system documentation

Requirements of ISO 17065 shall apply.

8.3 Control of Documents

Requirements of ISO 17065 shall apply.

8.4 Control of records

Requirements of ISO 17065 shall apply.

8.5 Management review

Requirements of ISO 17065 shall apply.

8.6 Internal audits

Requirements of ISO 17065 shall apply.

8.7 Corrective actions

Requirements of ISO 17065 shall apply.

8.8 Preventive actions

Requirements 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 CB and its clients and applicants

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

1. Maintaining documentation of tasks and responsibilities by the accredited certification body, for the purpose of
    a. responding to 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 providing information on the status and outcome of an application.

9.3.2 Communication between CB and the ICO

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

- of details of applicant on receipt of application to enable the ICO to check its records for the applicant's compliance history as per section 7.6 of this document;
- of the reasons for granting/withdrawing certification pursuant to Article 43.5, immediately prior to issuing, renewing, suspending or withdrawing certifications as per section 7.1(2) of this document.