ACCREDITATION REQUIREMENTS

APPLICABLE TO CERTIFICATION BODIES FOR THE CERTIFICATION MECHANISMS APPROVED UNDER ARTICLE 42 OF THE GENERAL DATA PROTECTION REGULATION

This content is a courtesy translation of the original publication in French. In the event of any inconsistencies between the French version and this English translation, please note that the French version shall prevail.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

1. To whom this document is aimed at?

This document is aimed at certification bodies referred to in Article 8 of the French Informatique et Libertés Act that are willing to obtain an accreditation to certify on the basis of the criteria of a certification mechanism approved pursuant to Article 42 of the General Data Protection Regulation (GDPR).

2. Scope of this document

This document defines the requirements that the certification body shall observe to obtain, and then maintain, its accreditation.

It constitutes the general framework for certification that apply to certification mechanisms that are approved pursuant to Article 42 when it has been decided, in accordance with the cooperation agreement signed between the CNIL and French national accreditation body (COFRAC), that the COFRAC is accrediting the certification bodies. In that case, the accreditation delivered by the COFRAC is the accreditation referred to in Article 43 of the GDPR.

This general framework can be supplemented by the application of conditions that are specific to a certification mechanism. In that case, the rules that are specific to a certification mechanism particularize the requirements of this document for the evaluation of the certification bodies.

This document is not applicable when the CNIL decide to conduct the accreditation of the certification bodies, in full or in part.

3. Accreditation procedure

The certification body shall submit an application file for accreditation to the COFRAC.

The application file defines the scope of the accreditation application by indicating the certification mechanism approved under article 42 to RGPD for which the certification body wishes to deliver certifications.

During the transitional period between the file application and the issuance of the accreditation, the certification body is authorized to start its certification activities provided that it has received from the COFRAC a positive outcome of the review of its accreditation application, called operational admissibility in accordance to the accreditation rules of the COFRAC.

This transitional period may not exceed 12 months: the certification body has a 12-months period, starting from the date it receives a positive answer from the COFRAC, to get accredited.
The cooperation agreement signed between the CNIL and the COFRAC on May 20th 2020 establish the roles, responsibility and the operational procedures regarding the accreditation of the certification bodies for the certification mechanisms approved under article 42 of the GDPR.

4. Validity period of the accreditation

The validity period of the accreditation is the one defined by the accreditation granted by the COFRAC.

5. Obligations of the certification body

To be accredited, the certification body shall:

- (1) demonstrate to the COFRAC that it complies with the requirements defined in the chapter 6 of this document;

- (2) establish a procedure to investigate and respond, in written form and without undue delay, to any request for information made by the CNIL regarding the provision of aggregate data related to its certification activity (statistics) or of records regarding the compliance to the accreditation requirements of this document, including the requirements related to the processing of complaints and appeals related to its certification activities.

It shall inform the COFRAC:

- (3) if is subject to, or has been subject to, investigations, sanction decisions and/or corrective measures imposed by the CNIL or other competent supervisory authorities under GDPR;

- (4) of any other binding decision that may constitute a non-conformity to the requirements of this document, including the decisions of the competent judicial authorities;

- (5) of any significant changes of its legal situation or any other situations affecting its certification activities that are might call into question its compliance to the requirement of this document;

- (6) other changes, prior to implementation, when the certification scheme introduces new rules that may substantial changes the conditions of the accreditation (e.g. substantial changes in the evaluation methods) or when the criteria of the certification mechanism are updated.

It shall inform the CNIL:

- (7) before it starts operating an approved European Data Protection Seal approved by the European Data Protection Board in a new Member State from a satellite office. In that case, the certification body shall also notify the competent supervisory authority of this Member State.
- It is also subject to the following obligations:
- (8) if the accreditation is suspended, the certification body is not authorized to issue new certificates until the suspension decision is lifted by the COFRAC. In the meantime, the certification body shall nonetheless continue its surveillance activity of the valid certifications;

- (9) If the accreditation is revoked, in case the certification body decides to resign its accreditation or have discontinued its certification activities, or when the certification body has been authorized to start its certification activities based on the operational admissibility received from the COFRAC but failed to get its accreditation granted by the COFRAC in due time, the certification body is not authorized to issue new certificates. The certificates already issued by the certification body remain valid for a period of six months. The certification body informs the organizations that hold a valid certificate (certified client) and the applicants in the certification process. These organizations choose another accredited certification body, or in the accreditation process of the COFRAC, to transfer their certification.

6. Requirements to be demonstrated by the certifcation body

Additional accreditation requirements Certification mechanism approved under article 42 of the GDPR Version 22-09-2022
1. Scope
This document defines requirements related to the competencies, the coherence of the activities and the impartiality of certification bodies operating a certification mechanism approved by the CNIL or by the European Data Protection Board pursuant to Article 42(5) and Article 43(2) b) of the General Data Protection Regulation (GDPR).

The nature of the data processing operation in scope of the certification mechanism (for example, a certification applicable to cloud service processing operations) shall be taken into account during the accreditation process of the certification body. For instance, it includes taking into account the type of processing operations the criteria apply to, the adequate competence required to perform the certification activities and the relevant evaluation methods to assess the conformity to the criteria.

For this purpose, a certification scheme might refine the requirements of EN ISO/IEC 17065 or the requirements of this document, for specific areas of application of the certification mechanism. The requirements of this document refer to the rules that might be defined to the certification scheme and apply to certification bodies for their accreditation.

2. Normative references

EN ISO/IEC 17065:2012: «Conformity assessment — Requirements for bodies certifying products, processes and services » (refer to as « ISO 17065 » in this document).

By default, all requirements of the ISO 17065 standard apply. The additional requirements of this document define specific requirements related to the evaluation of personal data processing carried out by a data controller or a data processor, pursuant to Article 43(1) b) of the GDPR.

GDPR has precedence over ISO 17065. However, the additional requirements defined in this document shall not contradict the rules related the organization and operation of the accreditation of certification bodies performing conformity assessment activities as defined the European Regulation (EC) 765/2008 of the European Parliament and of the Council of 9 July 2008.

If reference is made to other ISO standards in the scheme of a certification mechanism approved by the CNIL or by the EDPB, 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 [1] and certification [2] apply. They complement the terms and definitions of the EN ISO/IEC 17065:2012 standard.

For ease of reference the main definitions used in this document are listed below.

GDPR: 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

French Informatique et Liberté Act: Act no. 78-17 of 6 January 1978, amended, on information technology, data files and civil liberties

EDPB: European Data Protection Board

CNIL: The Commission nationale de l'informatique et des libertés (the Competent supervisory authority within the scope of this document)

Certification mechanism: compliance tool allowing a data controller or a data processor to be certification in relation to it is personal data processing operations

Scope of the certification mechanism: personal data processing operations that meet the conditions for eligibility to the certification mechanism

Certification: assurance given by an independent certification body that the compliance to certification criteria has been demonstrated

Certification criteria: the auditable requirements against which a conformity assessment is performed. The certification criteria are to be approved by the EDPB or by the CNIL (approved criteria)

Certification process: activities from application through to granting and maintenance of the validity of the certification (ex: evaluation activities, surveillance, etc)

Audit: systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled

[1] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42018-accreditation-certification-bodies-under_fr
[2] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying_fr

Note 1: **internal audits** are conducted by are conducted by, or on behalf of, the organization itself Note 2: **Second party** audits are conducted by parties having an interest in the organization, such as customers, or by other individuals on their behalf
Audit plan (or evaluation plan) : description of the activities and arrangements for an assessment
Audit findings: results of the evaluation of the collected audit evidence against the certification criteria
Audit evidence: records, statements of fact or other information, which are relevant to the certification criteria and verifiable
Non-conformity: non-fulfilment of a certification criteria
Audit report (or evaluation report): document used to present the result of the evaluation, including audit findings and conclusions
Accreditation: attestation granted to certification body conveying formal demonstration of its competence to carry out the certification process and authorizing it to issue certifications
Certification body: conformity assessment body operating a certification mechanism by conducting the tasks of the certification process
Related body: body which is linked to the certification body by common ownership, in whole or part, and has common members of the board of directors, contractual arrangements, common names, common staff, informal understanding or other means, such that the related body has a vested interest in any certification decision or has a potential ability to influence the process.
Accreditation requirements: requirements to which the certification body shall comply when performing the certification process in order to be granted the accreditation and maintain it (the requirements defined by this document for the certification mechanisms approved under article 42 when the CNIL is the competent supervisory authority)
Scope of the certification activities (or accreditation scope): certification activities conducted by the certification body for which accreditation is sought or has been granted
Certification scheme (or certification program): certification system gathering requirements, rules and procedures applicable to a certification mechanism. The certification scheme includes the certification criteria, certain rules related to the application of the accreditation requirements and specific procedures related to the certification process, including regarding the audit methodology
Scheme owner: person or organisation responsible for developing and maintaining a specific certification scheme
Client (or applicant): data controller or data processor that has been granted certification or has applied for it to a certification body
Object of the certification (or target of evaluation): personal data processing operation, involved in a product, process or service as defined by EN ISO/IEC 17065:2012 standard, that a data controller or a data processor is applying to have evaluated and certified.
Scope of certification: activities conducted by the client (or by the applicant) that involve the object of the certification. The identification of the scope of certification allows the certification body to define the scope where the certification process applies (ex: locations of the activities, subcontracted data processing, etc).
Evaluation method: procedure implemented by the certification body to perform an assessment of the object of certification
Appeal: request from a client to a certification body for reconsideration of any adverse certification decision related to the status of its desired certification status.
Complaint: expression of dissatisfaction, other than appeal, by any person or organization to a certification body, and relating to its certification activities

Certification transfer: the recognition of an existing and valid certification, granted by one accredited certification body, by another accredited certification body, for the purpose of issuing its own certification

4. General requirements

4.1 Legal and contractual matters

4.1.1 Legal responsibility

4.1(1) In addition to the requirements in §4.1.1 of ISO 17065, the certification body shall have up-to-date procedures that take into account the legal responsibility to which it is subject when carrying out its duties set out in the terms of accreditation, including the compliance to the additional requirements defined in this document in accordance with article 43(1) b) of the GDPR.

In particular, the certification body shall be able to demonstrate that it has procedures and measures that are compliant with GDPR specifically for the processing of the personal data of its client as part of the certification process.

4.1.2 Certification agreement (between the certification body and its clients)

4.1.2(1) In addition to the requirements in §4.1.2 of ISO 17065, the certification body shall ensure that its certification agreements include commitments from the client regarding the following:

a) comply with the certification criteria and implement appropriate changes when the certification criteria are update, including when those changes are communicated by the certification body;

b) provide the certification body with all information and access to its data processing activities which are necessary to conduct the certification procedure pursuant to Article 42(6) of the GDPR, within the limits of its organizational and technical measures implemented to ensure that personal data processing operations are performed in accordance with the GDPR and the French Informatique et Libertés Act;

It includes provisions for having access to the documentation and records, having access to the relevant equipment, location(s), area(s), allowing interview of its personnel and having access to relevant information related to the its subcontractors;

c) make all necessary arrangements for the participation of the CNIL and the COFRAC to the evaluation the client as observers;

d) comply with applicable deadlines and certification procedures. The certification agreement shall stipulate that deadlines and certification procedures, resulting for example from the certification scheme, must be observed and adhered to;

e) inform the certification body in the event of significant changes in its actual or legal situation, significant changes in the data processing operations in the scope of the certification, any changes that may affect the compliance to the certification criteria or any changes with regards to the information displayed on the formal certification documentation as defined in §7.7 of this document (certificate);

f) inform without delay the certification body of infringements of the GDPR or to the French Informatique et Libertés Act when they are established by the CNIL or by a competent judicial authority, and if they are likely to constitute a non-conformity to the certification criteria;

g) allow the certification body to communicate to the CNIL:

- all information for granting or withdrawing certification, according to the requirements in §7.6 (Certification decision) of this document;

- upon request from the CNIL, all information related to the certification procedure, according to the requirements in §7.12 (Records) of this document.

4.1.2(2) The certification agreements shall also inform the client regarding the following:

a) the certification does not reduce the responsibility of its client to comply with the obligations of the GDPR and to the French Informatique et Liberté Act, and is without prejudice to the tasks and powers of the CNIL in line with Article 20-23 of French Informatique et Liberté Act;

b) the evaluation methods that will be applied by the certification body for the assessment of the target of evaluation, as defined in the requirements in §7.3(2) b) of this document;

c) the organisational measures and the procedures put in place by the certification body for complaint and appeal management, in accordance with Article 43(2)(d) of the GDPR. The certification body shall also ensure that the certification agreement includes commitments of the client to comply with the rules set out by these procedures regarding the investigation of complaints within the meaning of §4.1.2.2 of ISO 17065;

d) the applicable rules for the validity, renewal, suspension and withdrawal of the certification pursuant to Articles 42(7) of the GDPR, including rules related to intervals for re-evaluation or review of the certification in line with the requirement in §7.9 of this document;

e) the general consequences of the expiry of its accreditation, its suspension, withdrawal or non-issuance. The possible actions for the client to maintain the validity of its certification or to renew its certification are also stipulated.

In particular, the client is informed of the general conditions applicable to the transfer of the certification and of the procedure to be followed in case the certification body is subject to a refusal, suspension or to a withdrawal decision of its accreditation for an approved certification mechanism under Article 42.

4.1.3 Use of licence, certificates and marks of conformity

4.1.3(1) In addition to the requirements in §4.1.3 of ISO 17065, the certification body shall exercise the control over the use and display of licenses, certificates, marks of conformity, and any other mechanisms for indicating a product, a service or a process is certified by ensuring that:

a) the certification mechanism is clearly referenced and, where applicable, the subset of the criteria applicable to the target of evaluation is indicated. In particular, communications shall be transparent about the type of data processing operations covered by the certification criteria when the certification mechanism applies to a specific subject-matters;

b) the scope of the certification is unambiguous to prevent any confusion about which data processing activities have been evaluated;

c) the rules of use of the mark owned by the CNIL and to be used by certified clients are applied.

Note: In the case of general certification mechanism, only a subset of the criteria might be applicable to some targets of evaluation. For instance, if the scope of the certification mechanism allows both data processors and controllers to apply for certification, the set of criteria applicable to the target of evaluation of a data controller will be significantly different from the set of criteria applicable when the processing operations of the target of evaluation are to be carried out by a data processor on behalf of a controller.

4.1.3(2) Incorrect or ambiguous use of licenses, certificates, marks of conformity and any other mechanisms for indicating a product, a service or a process is certified, shall be corrected with by suitable actions. It includes at least:

a) the obligation for the client to take any measure to put an end to the incorrect or misleading practices;

b) the obligation for the client to renew the information of the public, by default, using communication means similar to ones previously used;

c) informing the CNIL, without undue delay, about non-compliant practices that have be observed and the actions taken by the certification body and the client.

Note: Other suitable actions decided by the certification boy may also include suspension or withdrawal of the certification, publication of the transgression and, if necessary, legal action.

4.2 Management of impartiality

4.2(1) In addition to the requirements in §4.2 of ISO 17065, the certification body shall provide evidence of:

a) its independence in line with Article 43(2)(a) of the GDPR. It includes evidence concerning the financing of the certification body in so far as it concerns the assurance of impartiality;

b) that its tasks and duties do not lead to a conflict of interest pursuant to Article 43(2)(e);

c) that it has no relevant connection with the clients it assesses.

Note : In addition to requirements of this document aiming at preventing the conflict of interest, the requirements of §4.2 and §5.2 of ISO 17065, related to management of identified conflicts of interest, apply. In particular, the certification body shall identify risks to its impartiality on an ongoing basis and shall take actions to respond to any risks to its impartiality, arising from the actions of other persons, bodies or organizations, of which it becomes aware.

4.2(2) In particular, the certification body shall ensure for each of its clients that:

a) its personnel involved in the evaluation, review and decision-taking procedures for the certification do not have other link with its client than its certification activities and do not have other activities in relation to the object of the certification that would call the impartiality of the certification body;

b) its client is not a related body (or a relationship as defined in §4.2.3 of ISO 17065) that presents a risk of impartiality to the certification body;

c) it did not have economic relationship with its client during the last 2 years (except the one settled by a certification agreement) and is not financed by its client for other activities than the certification. In particular, the certification body shall not outsource the processing of its personal data to its client.

4.3 Liability and financing

4.3(1) In addition to the requirement in §4.3 of ISO 17065, the certification body shall have adequate arrangements (e.g. insurance or reserves) to cover its liabilities arising from its operations in the geographical regions in which it operates the certification mechanism.

4.4 Non-discriminatory conditions

4.4(1) In addition to the requirements in §4.4 of ISO 17065, the certification body shall be transparent with all applicants about:

a) the type of personal data processing in the scope of the certification mechanism that fall within the scope of its certification activities (accreditation scope);

In particular, when the certification body does not have adequate evaluation methods for the evaluation of data processing operations of a specific sector of activities (for instance, when the evaluation involves the processing of special categories of personal data or when technologies specific to a sector are used) or when its personnel does not have the appropriate competencies to conduct the evaluation of a type of a data processing operations, the certification body shall inform the applicants about such limitations and provide a list of the sectors of activities in the scope of it evaluation activities for the certification mechanism;

b) the list of Member States of the European Union that fall within the scope of its certification activities, for a transnational certification mechanism approved by several SAs and for a European data protection seal approved by the EDPB;

In particular, when the certification body does not have adequate evaluation methods for the evaluation of data processing operations subject to a specific national data protection law of a Member State of the European Union or when its personnel does not have the appropriate competencies to

conduct the evaluation in the context of a specific national data protection law of a Member State, the certification body shall inform the applicants about such limitations and provide a list of the Member States of the European Union in the scope of it evaluation activities for the certification mechanism.

4.5 Confidentiality

4.5(1) In addition to the requirements in §4.5 of ISO 17065, the certification body shall inform the client about the information to be provided to the CNIL for the need of the certification process. It includes the following information:

a) the certification decisions (see the requirements in §7.6 of this document);

b) the information to be submitted to the CNIL regarding the registry of certifications (see the requirements in §7.8 of this document).

4.5(2) The certification body shall inform the client that, upon request from the CNIL, it may provide to the CNIL additional records related to its evaluation to demonstrate the compliance of the certification process against the requirements in this document (see the requirements in §7.12 of this document), including contractually confidential matters related to data protection compliance.

In particular, the certification body shall not collect confidential information for which the client might rightly claim that they cannot be released to the members and agents of the CNIL in carrying out their duties due to the conditions of secrecy strictly defined in article 19 III of the French Informatique et Liberté Act: information covered by the professional secrecy applicable to the lawyer-client relationship, the secrecy of journalists' sources and the medical secrecy.

4.5(3) The certification body shall inform the client that the CNIL has the investigative power to carry out a review on certifications issued pursuant to Article 42(7) of GDPR. The conditions applicable to the exercise of the powers conferred on the CNIL pursuant to Article 58 are defined by the GDPR and French Informatique et Liberté Act and fall outside the scope of the requirements in this document.

4.6 Publicly available information

4.6(1) In addition to the requirements in §4.6 of ISO 17065, the certification body shall make accessible to the public:

a) all valid versions (current and previous) of the certification criteria that are currently in use in the issued certificates, stating their respective period of validity;

b) deprecated versions of the certification criteria that are no more in use in valid certificates, stating their respective period of validity;

c) the up-to-date certification procedures, including procedures for handling complaints and appeals pursuant to Article 43(2) d) of the GDPR;

d) information about how the certification procedures can be applied in practice, including information provided to the data subjects concerned by the personal data processing involved in the scope of the certification about how to lodge a complaint and how it will be handled by the certification body.

5. Structural requirements

5.1 Organizational structure and top management

5.1(1) Requirements in §5.1 of ISO 17065 shall apply.

5.2 Mechanism for safeguarding impartiality

5.2(1) Requirements in §5.2 of ISO 17065 shall apply.

6. Resource requirements

6.1 Certification body personnel

6.1(1) In addition to the requirements in §6.1 of ISO 17065, the certification body shall establish, implement and maintain a procedure for the management of competencies to demonstrate that its personnel has appropriate and ongoing expertise (knowledge and experience), pursuant to Article 43(1) of the GDPR, to properly perform the certification activities. In particular, the personnel shall:

a) have undergone a specific training on personal data protection; b) has relevant and appropriate knowledge about and experience in analysing and/or applying data protection legislation (GDPR, the French Informatique et Libertés Act and other national laws applicable to the scope of the certification mechanism); c) has relevant and appropriate knowledge about and experience in analysing and/or applying the technical and organizational data protection measures relevant to the scope of the certification mechanism pursuant to Article 43(2) a) of the GDPR; d) has appropriate expertise in the evaluation of data processing operations (audit). Note: The relevance and appropriateness of knowledge and experience shall be defined by the certification body so that each person involved in the certification process (application, evaluation, review, decision, monitoring, etc.) is able to achieve its tasks, taking into account the rules defined by certification scheme and the minimum requirements related to personnel competencies defined by this document. It includes taking into account specific needs for competencies related to the scope of the certification mechanism and/or to the target of evaluation that can be submitted for certification, for instance, for the specific sectors of activities that the certification mechanism applies to (e.g. cloud service), some specific categories of personal data (e.g. health data) or the specific technologies used by some services (e.g. website tracking technology).
6.1(2) The certification body shall ensure that the personnel in charge of evaluations has: a) undergone a training on audit methods (audit principles, audit procedures and techniques, documents relating to audits, rules and requirements applicable to audit, etc.); b) taken part in at least 2 full audits, from their preparation to the final conclusions, in the last three years. Note: Internal audits and second-party audits are accepted when the evaluation was conducted based on established requirements/internal rules and according to an audit procedure.
6.1(3) The certification body shall ensure that the personnel responsible for review and/or certification decisions has in-depth knowledge on and experience in: a) the state-of-the-art, risks and key issues relating to data protection; b) the performance of certification activities. Note: When the certification body assign a group of persons to take one certification decision according to §7.6.2 of ISO 17065 and if such personnel does not have the knowledge and experience required in §6.1(3) of this document, the certification process leading to this individual certification decision shall include a review process involving at least one person having the competencies required by the requirements in §6.1(3) of this document.
6.1(4) The certification body shall have personnel with legal and technical expertise whose profile meet: a) the technical profile requirements as defined in §6.1(5), §6.1(6) and §6.1(7) of this document; b) the legal profile requirements as defined au in §6.1(8) et §6.1(9) of this document. Note: Internship and apprenticeship periods are not work experience to be taken into account for demonstrating the required number of years of professional experience defined for the personnel in charge of conducting evaluations and responsible for the review, as defined by this document.
6.1(5) (Technical profile requirement) The certification body shall ensure that its personnel with technical expertise has obtained:

a) at minimum, a degree level qualification to at least EQF level 6 (bachelor's degree) ("Licence" in the French national qualifications framework) in the field of computer science, information systems or cybersecurity or a state-recognised protected title (e.g. Dipl. Ing.) in the same field; b) or have a significant professional experience of at least 5 years in the field of personal data protection. Note: The professional experience required in §6.1(5) b) of this document is an alternative to the degree or other recognised protected title required in §6.1(5) a) ("*Validation des Acquis de l'Expérience* – VAE" in the context of this document). This professional experience can also be taken into account, when relevant, to meet other requirements regarding professional experience of this document.
6.1(6) (Technical profile requirement) The certification body shall ensure that its personnel with technical expertise has undergone at least a 2 days training on applicable information system security management (regulation, standards, methods, best practices, risk management, etc.).
6.1(7) (Technical profile requirement) The certification body shall ensure that its personnel with technical expertise has appropriate and ongoing expertise that includes: a) for the personnel in charge of conducting evaluations, at least 2 years of professional experience in data protection, such as analysing and/or implementing technical and organizational data protection for information systems and that is relevant to the scope of the certification mechanism (e.g. security measures tests, technical evaluation procedures or certifications); b) for the personnel responsible for the review of the certification (or for taking decisions), at least 2 years of professional experience in identifying, defining, monitoring data protection measures or giving advice in the data protection domain.
6.1(8) (Legal profile requirement) The certification body shall ensure that its personnel with legal expertise have obtained: a) a degree level qualification ("Niveau Master 1" in the French national qualifications framework) in the legal field or an equivalent EU state-recognised qualification for at least eight semesters including the academic degree Master (LL.M.); b) or have a significant professional experience of at least 5 years in the field of personal data protection. Note: The professional experience required in §6.1(8).b of this document is an alternative to the degree required in §6.1(8).a ("*Validation des Acquis de l'Expérience* – VAE" in the context of this document). This professional experience can also be taken into account, when relevant, to meet other requirements regarding professional experience of this document.
6.1(9) (Legal profile requirement) The certification body shall ensure that its personnel with legal expertise has appropriate and ongoing expertise that includes: a) for personnel in charge of conducting evaluations, at least 2 years of professional experience in data protection law, such as analysing and/or implementing the compliance of personal data processing operations to the applicable laws (e.g. contracts reviews or audit of procedures related to data subject rights); b) for the personnel responsible for the review of the certification (or for taking decisions), at least 2 years of professional experience in monitoring data protection compliance or giving advice in the data protection domain.
6.1(10) The certification body shall ensure that is personnel maintain its competencies, for instance through continuous professional development.
6.1(11) In addition to the requirement in §6.1.3 of ISO 17065, the certification body shall require the personnel involved in the certification process to commit themselves to comply with the rules defined by the certification body relating to the independence of its personnel from commercial and other interests with regards the object of certification pursuant to Article 43(2)(a) of the GDPR.

The certification body shall use this information as input into identifying risks to impartiality raised by the activities of such personnel, or by the organizations that employ them pursuant to §4.2.3 of ISO 17065 and to demonstrate that their tasks do not raise a conflict of interest pursuant to Article 43(2) e) of the GDPR.

6.2 Resources for evaluation

6.2(1) In addition to the requirements in §6.2 of ISO 17065, the certification body shall ensure that the body it mandates to provide outsourced services for its evaluation activities, and the personnel that it uses to conduct the evaluation activities, meet the requirements of this document related to the evaluation activity.

As required in §6.2.2.4 and in §7.6.1 of ISO 17065, the certification body shall take responsibility for all activities outsourced to another body and shall be responsible for, and shall retain authority for, its decisions relating to certification.

6.2(2) In particular, when parts of the evaluation activities are outsourced to external bodies, the certification body shall:

a) check, for each person in charge of conducting evaluations, that the requirements in §6.1 of this document are fulfilled;

b) control that the personnel involved in the evaluation process does not have other link with the client than the certification process or other activities related to the client's activities that would call the impartiality of the certification body (see requirements in §4.2 of this document).

7. Process requirements

7.1 General

7.1(1) Requirements in §7.1 of ISO 17065 shall apply.

The personal data processing operations shall be evaluated against the certification criteria approved by the CNIL pursuant to Article 58(3) of the GDPR and Article 8(I)(2°) h) of the French Informatique et Libertés Act or by the EDPB pursuant to Article 63 of the GDPR.

Note: When performing its evaluation activities, the certification body should take into account the guidance and the proposed evaluation methods or testing methods provided by the scheme owner.

7.2 Application

7.2(1) In addition to the requirements in §7.2 of ISO 17065, the certification body shall obtain the following information from the applicant with respect to the object of the certification:

a) a detailed description of the target of evaluation, including its interfaces with other systems and/or organizations. In particular, underlying protocols as well as assurance related to these interfaces allowing data communication between the object of certification and external systems and/or third-party organization shall be provided;

b) the list of the data transfers to an organization located in a third country (outside the European Union) or to an international organization. The national law applicable to the data recipient and the type of data protection safeguards shall be provided;

c) the responsibilities, data processing activities and/or tasks of the applicant, when the applicant is a data processor or a joint-controller;

d) the list of the data processors (or data sub-processors when the applicant is a processor). Their responsibilities and data processing activities shall be described and the main contracts or contractual templates that binds the applicant and its processors shall be identified;

e) the list of joint controllers. Their responsibilities and tasks shall be described and the principles of the binding arrangements with the applicant shall be provided (or the nature of the legal instruments used);

f) the general characteristics of the data processing operations in the scope of the certification, including the address(es) of the physical location(s) of the applicant where data are processed, the categories of data involved and the national legal obligations applicable to the data processing operations;

g) where appropriate, the information about certifications or other evaluation results completed prior to the application, when the nature of these evaluations and their scope may be considered in the certification process;

h) the existence of ongoing investigations, or recent sanction decisions and/or corrective measures imposed by the CNIL or other competent supervisory authorities to the applicant, when they involve personal data processing operations in the scope of the certification.

7.3 Application review

7.3(1) When conducting the application review as required in §7.3 of ISO 17065, the certification body shall consider all the information referred in §7.2 of this document.

7.3(2) In addition to the requirements in §7.3.1 of ISO 17065, the certification body shall conduct a review of the collected information to ensure that:

a) the object of certification is a fit candidate to the evaluation against de certification criteria, taking into account the rules defined by the certification scheme. In particular, the certification body shall ensure that the applicant and the data processing operations submitted for certification fall within the scope of the certification mechanism regarding:

- the responsibilities of the applicant for the proposed object of certification with regards to the applicable data protection laws (data controller, joint-controller, processor, sub-processor, etc);

- the type of data processing operations related to the object of certification, taking into account the data processing operations for which the certification criteria have been designed and approved pursuant to Article 42 of the GDPR;

b) it has evaluation methods appropriate to the target of evaluation, taking into account:

- the rules defined by the certification scheme related to the evaluation methods to be applied for assessing the compliance of the processing operations to the certification criteria;

- the data protection laws applicable to the target of evaluation;

- the ongoing investigations, or recent sanction decisions and/or corrective measures imposed by the CNIL or other competent supervisory authorities to the applicant;

The certification body shall describe the evaluation methods used for evaluating the compliance of the processing operation to the certification criteria in a consistent manner, meaning that comparable evaluation methods are used for the evaluation of comparable target of evaluation and will lead to comparable results;

c) it has both the appropriate technical and legal expertise in data protection, as required in §6 of this document, to perform the certification activity, in particular when the certification body has no prior experience in the assessment of the same type of object of certification or of a similar scope of certification.

7.3(3) When the certification scheme defines rules for the calculation of the duration for the evaluation activities (e.g. in days), the certification body shall implement a procedure to perform the audit time calculation. This procedure shall take into account the following factors for the application of the evaluation methods:

a) the scale of the personal data processing operations in the scope of certification;

b) the nature of the personal data processed;

c) the risks of the data processing operations for the data subjects;

d) the complexity of the assessment of the technologies used for the data processing operations;

e) the use of data processors to perform the processing;

f) the numbers of structures/site of the applicant in which the personal data processing activities are performed.

When the certification scheme defines rules for the calculation of a (minimal) duration for the evaluation of the client, the certification body shall calculate this audit time as specified by the certification scheme and determine whether the calculated audit time is sufficient to achieve its tasks or if it shall be extended. The certification body keep record of the adopted duration.

The audit time defined by the certification body shall be stipulated in the contractual agreement.

7.3(4) When the application is submitted by an applicant willing to change its certification body by asking a certification transfer, the certification body shall follow the applicable rules defined by the certification scheme.

In particular, the certification body shall:

a) ensure that the applicant hold a certificate that is valid by the time of his application;

b) in addition to the information listed in §7.2 of this document, obtain from the applicant:
- a copy of the issued certificate,
- the last evaluation report,
- the complaints received;

c) in addition to the review conducted according to §7.3(2) of this document, analyse, by a document review, the status of the pending non-conformities, the findings of the last evaluation report, the complaints received and the corrective actions;

d) take its decision regarding the certification transfer within a delay of 1 month.

Note: if all or part of these documents are not obtained from the applicant or if there is a doubt about the compliance of the target of evaluation to the certification criteria, the certification body shall not transfer the certification as it is and shall start the certification process from the beginning (initial certification), as provided in §7.4 of this document.

7.4 Evaluation

7.4(1) In addition to the requirements in §7.4 of ISO 17065, the certification body shall have a plan for the evaluation activities (audit plan). The audit plan shall allow to apply the evaluation methods laid down in the contractual agreement according to §4.1.2(1) b) of this document.

The application of the evaluation methods may require an evaluation in the client's premises in order to collect the relevant findings that demonstrate compliance to the certification criteria. Any deviation from the evaluation methods shall be justified by the certification body.

7.4(2) The certification body shall apply the evaluation methods laid down in the contractual agreement during the evaluation, for example by applying:

a) a method for assessing the necessity and proportionality of processing operations in relation to their purpose and the safeguards for the rights and freedoms of the data subject;

b) a method for evaluating the coverage, the type and assessment of all risks considered by the controller and the processor with regard to their obligations pursuant to Articles 30, 32 and 35 and 36 of the GDPR, and with regard to the appropriateness 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;

c) a method for assessing the remedies, including guarantees, safeguards and procedures to ensure the protection of personal data for the processing activity involved in the target of evaluation.

7.4(3) The certification body shall assign personnel with appropriate competencies to perform the evaluation tasks, taking into account the rules defined by the certification scheme. The certification body shall ensure that all personnel involved in the evaluation tasks, whether internal or outsourced resources, meet the requirements related to competencies, as defined in §6 of this document.

In particular, for each evaluation, the certification body shall ensure that the evaluation team, as a whole, has both legal and technical expertise as required in §6 of this document.

In exceptional circumstances, when the certification body assign to the evaluation tasks a person who does not meet the "technical profile" nor the "legal profile" requirements (as defined in §6 of this document), it shall justify the need for assigning an "expert" with specific competencies for the need of a particular evaluation (e.g. personnel specialized in a specific technology or in a specific sector of activity involving the processing of special categories of personal data or for which specific national laws are applicable). In that case, the results of the evaluation tasks performed by the person with an "expert" profile shall be supervised during the evaluation process by the personnel in charge of conducting the evaluation that meet the "technical profile" or the "legal profile" requirements (e.g. the auditor leading the audit team).

7.4(4) In addition to the requirements in §7.4.5 of ISO 17065 and as part of the review process required in §7.3 of ISO 17065, when the certification body relies on the evaluation results related to a certification completed prior to the application, the certification body shall:

a) make sure that the certificate will be valid at the time of the evaluation and that the certification is relevant regarding the target of evaluation;

b) document how and to what extend the results related to the certification that was obtained beforehand can be considered for the evaluation of the certification criteria, taking into account the rules defined by the certification scheme;

c) determine the consequences for the remaining evaluation to be done and on the evaluation methods to be applied, e.g. by defining a correspondence matrix between the criteria of the two certification mechanisms in the context of the target of evaluation.

7.4(5) When taking responsibility for the results related to certification completed prior to the application, the certification body shall ensure the compliance of the target of evaluation to all criteria of the approved certification mechanism. In particular, the certification body shall:

a) have access to the full assessment report of the certification obtained beforehand (and not only to the certificate or similar attestations);

b) document its own findings by:

- referring to the relevant results available in the existing certification report (copy-pasting existing results is not required);

- making all additional findings when are necessary to the evaluation of the commentary criteria of the approved certification mechanism.

If deviations from the results related to an existing certification are identified by the certification body during the evaluation of the criteria of the approved certification mechanism, the evaluation shall be extended to the impacted criteria and, if necessary, on the entire target of evaluation already certified.

7.4(6) In addition to the requirements on §7.4.6 of ISO 17065, the certification body shall define in its certification procedures how the client is informed of the results of the evaluation, including non-conformities, taking into account the rules defined by the certification scheme, including the form and timing of the provision of such information to the client.

7.4(7) In addition to the requirements in §7.4.9 of ISO 17065, the certification body shall document findings, for each certification criterion, according to the rules defined by the certification scheme. As a minimum, the evaluation report shall include:

a) the description of the target of evaluation;

b) the evaluation plan (including updates made during the evaluation);

c) references to the documents and records that have been examined;

d) references to the data processing operations that have been evaluated;

e) the functions of the persons that have been interviewed;

f) the physical location(s) of the applicant where the findings were made;

g) a description of non-conformities that identifies the certification criteria that are not-fulfilled and evaluates the severity and the extend of the non-compliance.

The certification body invite its client to propose the implementation of corrective measures to handle non-conformities, so that they can be taken into account by the certification body when taking its certification decision (see requirements in §7.6 of ISO 17065). The action plan resulting from the certification decision shall also be annexed to the evaluation report. This action plan shall be analysed by the certification before the review and the certification decision.

7.4(8) The certification body shall provide to the CNIL, upon request, the reports of its evaluation and their annexes.

Note: For the purpose of demonstrating the compliance to the requirements of this document, the certification body is not required to keep the supporting documents related to audit findings documented in the audit report (e.g. document samples, screen captures, log files, etc).

Note: According to requirements in §7.12 of this document, the certification body shall keep the evaluation report and its annex available for a period of 6 years.

7.4(9) If the personal data involved in the scope of the certification are processed from several structures/site of the applicant, the evaluation shall be conducted according the rules defined by the certification scheme regarding multi-site certification.

When a non-conformity is identified for one of these structures/sites, the certification body requires its client to:
- analyse the extend and the causes of the non-conformity; and
- propose the implementation of preventive measures so that the non-conformity does not repeat in other locations of the client.

This analysis and the proposed preventive measures are included in the action plan referred to in §7.4(7) of this document and are reviewed by the certification body.

7.5 Review of the results of the evaluation activities

7.5(1) In accordance to the requirements in §7.5 of ISO 17065, the certification body shall review all information and results related to the evaluation.

In addition to the requirements in §7.5 of ISO 17065, the review process shall be defined, taking into account the rules defined by the certification scheme. In particular, the certification body shall:

a) check that the scope of certification is consistent with the object of the certification that was evaluated;

b) check that the evaluation methods have been followed and that audit findings available in the evaluation report are relevant.

7.5(2) The certification body shall assign personnel with appropriate competencies to perform the review tasks, taking into account the rules defined by the certification scheme. The certification body shall ensure that all personnel involved in the review tasks, whether internal or outsourced resources, meet the requirements related to competencies, as defined in §6 of this document.

In particular, for each review, the certification body shall ensure that the personnel responsible for the review have both legal and technical expertise as required in §6 of the current document.

7.6 Certification decision

7.6(1) In addition to the requirements in §7.6 of ISO 17065, the certification body shall define procedures for taking certification decisions or refusing the certification, taking into account the rules defined by the certification scheme.

The certification body shall also define procedures for taking other decisions related to the certification when an evaluation has been conducted in the context of the surveillance activities as defined in the requirements in §7.9.2 of ISO 17065 or when the appropriate measures in response to a non-conformity include an evaluation pursuant to §7.11 of ISO 17065: renewing the certification, updating the scope of the certification (extending or reducing the scope), suspending (and reinstating) the certification and revoking the certification.

These procedures shall require that:

a) the reasons for taking a favourable decision are identified and documented with objective facts and evidence;

b) the reasons for refusing, suspending or withdrawing the certification are identified and documented, including with regards to the gravity, the number and the recurrence of the non-conformities;

c) the time period between the end of the evaluation (last documented findings) and the decision may not exceed 3 months, except in exceptional circumstances where justifications are documented;

d) in addition to the review of information carried out at the application stage (see requirements in §7.2(1) h) of this document), about any ongoing investigations, or recent sanction decisions and/or corrective measures imposed by the CNIL or other competent supervisory authorities to the client, the certification body shall verify with the client that this information is up-to-date prior taking a decision.

If new investigations have occurred or if corrective measures have been imposed to the client in the meantime, the certification body shall evaluate if it might entail non-compliance with the certification criteria and if it might prevent the certification from being issued (or renewed, reinstated or extended).

The certification body shall document in its evaluation report (and/or in its certification decision) its conclusions regarding such investigations or imposed corrective measures related to the personal data processing activities in the scope of the certification.

e) the certification body shall inform the CNIL of its decisions, in writing and before applying the decisions, when the certification is granted (renewed, reinstated or extended) or withdrawn (reduced or suspended) pursuant to Article 43(5) of the GDPR;

The information to be provided to the CNIL includes:

- the name of the client;

- the scope of the certification;

- the description of the object of certification;

- an executive summary of the evaluation report which explains how the criteria are met (or why they are no longer met);

- the draft formal certification documentation, as, referred to in §7.7.1 of ISO 17065 (the draft certificate);

f) The certification body shall inform the client of the certification decisions.

7.6(2) The certification body shall define its certification procedures to ensure its independence and responsibilities with regard to the certification decisions. In particular, the certification body shall demonstrate that the person(s) or the group of persons assigned to the certification decisions have not directly nor indirectly been involved in the evaluation process.

7.7 Certification documentation

7.7(1) In addition to the requirements in §7.7 of ISO 17065, the certification body shall provide the client with formal certification documentation (certificate) that allow to identify:

a) the name and reference (including version) of the certification criteria that were used for the evaluation;

b) the scope of certification, including a clear and comprehensible statement of the object of certification and of the list of the locations of the client where the personal data processing activities are performed;

When the applicability of a set of criteria relies on the context of the data processing involved in the scope of certification (e.g. the status of the applicant as data controller or processor, the processing of special categories of personal data, the use of specific technologies, the applicability to a specific sector of activity, etc.), the scope of the certification shall be described in such a way that the applicable subset of criteria that have been evaluated can be understood;

c) the object of certification (the target of evaluation), including its version or other relevant applicable identifiers.

7.7(2) The certification body shall provide its client with formal certification documentation (certificate) where the term or expiry date of certification is set according to the period of validity of the certification defined by the certification scheme. The certification body shall ensure that the period of validity of a certification does not exceed 3 years.

7.8 Directory of certified products

7.8(1) In addition to the requirements in §7.8 of ISO 17065, the certification body shall maintain information on the certified target of evaluation, according to the rules defines by the certification scheme, which includes at least:

a) the scope of certification;

b) a clear and comprehensible statement of the object of certification (a meaningful description of the target of evaluation), including its version or other relevant applicable identifiers;

c) the name and/or reference (including version) of the certification criteria that were used for the evaluation;

d) the status of validity of the certification: pending (not yet issued), granted (initial certification), renewed, expired, resigned, suspended or withdrawn;

e) the date certification was granted (or renewed);

f) the dates surveillance activities were conducted;

g) the term or expiry date of certification, or the date certification was resigned, suspended or withdrawn.

Note: this information includes a record of actions achieved by the certification body for each certified target of evaluation. It does not have to be made public unless stipulated by the certification scheme, contrary to the information detailed in §7.8(2) of this document which aim at making available to the public a list of the target of evaluation whose certificate is valid. However, it shall be made available upon request to third parties that wish to make sure of the validity of a given certification, for instance, within a specific period of time in the past or for a target of evaluation that has changed over time.

Note: According to requirement §7.12 of this document, the certification body shall keep the records of information on certified objects for a period of 6 years.

7.8(2) The certification body shall provide to the public an executive summary of the certification decision documentation in order to help with transparency around what is certified and how it was assessed. The information to be published is defined by the certification scheme.

The certification shall, as a minimum, publish in a directory an executive summary that includes:

a) the name of the client and contact details;

b) the scope of certification, including a clear and comprehensible statement of the object of certification;

c) the object of certification (the target of evaluation), including its version or other relevant applicable identifiers;

d) the name and/or reference (including version) of the certification criteria that were used for the evaluation and, if any, the specificities of the evaluation methods used to assess the compliance of the processing operation(s) to the certification criteria;

e) the date certification was granted (or renewed);

f) the status of validity of the certification which results from the last certification decision.

When informing the CNIL before the certification is granted (pursuant to the requirement in §7.6 of this document), the certification body shall provide to the CNIL the above information that will be published. The scope of certification and the object of certification shall be provided to the CNIL in French language

7.9 Surveillance and Renewal

7.9(1) The certification body shall define procedures to review the conformity of the certified target of evaluation against the certification criteria pursuant to article 43(2) c) of the GDPR.

In addition of the requirements in §7.9 of ISO 17065, the surveillance shall include:

a) an evaluation of the changes that were applied to the data processing operations in the scope of the certification since the last evaluation and their potential impacts on the conformity to the certification criteria;

b) an evaluation of the certification criteria for which the implementation modalities were evaluated during the previous audit but for which the actual implementation was not yet applicable (e.g. due to the fact that some data processing operations that had not started);

c) an evaluation of the implementation of data protection measures identified by the action plan resulting from the previous certification decision (see requirements in §7.4 and §7.11 of this document);

d) an in-depth evaluation of a defined set of criteria that are selected taking into account the risks of non-conformity that were observed during the previous evaluations (but did not lead to an established non-conformity). For instance, the evaluation can be deepened by:

- analysing more records (e.g. files, contracts, interviews, etc.) to strengthen the previous findings;

- analysing the recent records in the scope of certification to ensure that the previous findings are still valid over time: the evaluation of the compliance of the certification criteria for one or several new data processing operations in the scope of the certification since the last evaluation;

- analysing the data processing activities in different contexts included in the scope of certification (e.g. an evaluation in other physical locations of the client, of some personalized service or process, etc) to ensure that findings are consistent.

7.9(2) The certification body shall plan its surveillance activity according rules defined by the certification scheme. The maximum period between surveillance activities should not exceed 12 months.

In addition to regular evaluations, the monitoring measures required to maintain the certification shall:

a) ensure that the information related to the certification is up to date (e.g. description of the target of evaluation);

b) enable the planning of complementary evaluations initiated by the certification body, where proportionate to the risks for data protection. For instance, a complementary evaluation may occur when non-conformities are suspected due to one or more complaints received by the certification body or on the basis of information about non-conformant practices that have been publicly disclosed or when required to provide the CNIL with requested information related to the compliance to the accreditation requirements of this document.

7.9(3) The certification body shall document the results of its surveillance activity for each certification, including its consequences when the surveillance activities lead to a decision to reduce the scope of the certification, to suspend or withdrawn the certification.

Note: According to requirement §7.12 of this document, the certification body shall retain records of its surveillance activity for a period of 6 years.

7.9(4) When the application of the client is the renewal of a certification, the certification body shall follow a certification process that meet the same requirements of this document that are apply to the initial certification request.

The certification body shall follow the specific rules defined by the certification scheme related to the renewal of certification. In particular, it may include rules regarding the issuing of certificates (e.g. the date the certification is renewed).

7.9(5) When the scope of certification includes several structures/sites of the client, the certification body shall apply the rules defined by the certification scheme regarding the consequences for the certification process of the addition of locations (extension of the scope of certification) or their termination (reduction of the scope of certification).

In particular, the certification body shall define the plan for its evaluation activities of the structures/sites of the client over the period of validity of the certification.

7.10 Changes affecting certification

7.10(1) In addition to the requirements in §7.10 of ISO 17065, changes affecting certification to be considered by the certification body shall include:

a) any infringement of the GDPR or the French Informatique et Libertés Act reported by the client to the certification body in relation to the object of certification;

b) any change in the personal data processing operations reported by the client as likely to affect the compliance of the object of certification to the certification criteria;

c) any amendment to the personal data protection legislation in relation to the scope of the certification mechanism;

d) the adoption of delegated acts of the European Commission in accordance with Articles 43(8) and 43(9) of the GDPR in relation to the scope of the certification mechanism;

e) decisions or binding opinions of the EDPB and/or the CNIL in relation to the scope of the certification mechanism;

f) court decisions related to personal data protection in relation to the subject-matter that is brought to its attention in relation to the subject-matter of the certification;

g) new developments in the state of the art of technology employed for data processing operations;

h) emerging risks for data protection.

Note: the certification body should also take into account the recommendations and best practices adopted by the EDPB and/or the CNIL in relation to the subject-matter of the certification mechanism.

7.10(2) The certification body shall define a procedure in order to analyse, decide and implement changes affecting the certification process, taking into account the rules defined by the certification scheme. As a minimum, it shall include:

a) establishing and maintaining a record of the changes that were analysed as affecting the certification process and identifying the impacted targets of evaluation;

b) documenting the actions decided to implement the changes affecting certification, in particular:

- the immediate complementary evaluation or re-evaluation of the certification criteria;

- the rationale that lead to not conducting an immediate complementary evaluation or re-evaluation of the certification criteria for the impacted targets of evaluation;

- the rationale that lead to not conducting any evaluation and, if so, the other types of actions that were performed;

- the rules applicable to transition periods, including when defined by the scheme owner in the context of the update of the certification criteria, the deadlines for the evaluation of the changes to be performed and the conditions for maintaining or renewing the certification of impacted targets of evaluation;

c) informing the client, in a timely manner, when changes affecting its certification will lead to an evaluation and what need to be evaluated (and how) to ensure that the certified processing operations in the scope of the certification are still in compliance with the certification criteria. The planned evaluation shall be proportionate to the consequence on the certification. If a transition period is defined, the client shall be informed of the deadlines to be respected to maintain or renew its certification, as well as the consequences if they are not respected;

d) revising the formal certification documentation (certificates), suspending or withdrawing the certification, if the evaluation concludes that the data processing operations in the scope of the certification are no longer in compliance with the certification criteria;

e) update its certification procedures, including the relevant evaluation methods, taking into account the rules defined by the certification scheme, so that they apply to all future clients in a consistent manner.

7.10(3) In cases where the client informs the certification bodies of ongoing investigations, or recent sanction decisions and/or corrective measures imposed by the CNIL or other competent supervisory authorities to the applicant that brings into question the client's compliance the applicable data protection rules, the certification bodies shall document the result of its assessment on whether the target of evaluation still conforms with the certification criteria, including its outcome when it leads to a certification decision.

7.11 Termination, reduction, suspension or withdrawal of certification

7.11(1) In addition to the requirements in §7.11 of ISO 17065, the certification body shall define procedures to handle nonconformity of the target of evaluation according to the rules defined by the certification scheme. As a minimum, it includes that:

a) when a nonconformity to the certification criteria is established, the certification body shall determine if the corrective measures proposed by the client are likely to solve the non-conformity before the certification decision is taken. This opinion is without prejudice of the conclusions of the evaluation of the implementation of the corrective measures by the client to be performed by the certification body;

For all non-conformities, the certification body shall evaluate if the action plan is appropriate to ensure the conformity of the data processing operations when taking its certification decision. If the action plan is not sufficient to ensure it, the certification body shall suspend its certification decision until evidence of the implementation of corrective actions is available;

b) the certification body shall define the delays for the application of the relevant corrective measures (action plan), taking into account the severity of each nonconformity;

c) when the certification is conditional on implementation of an action plan, the certification body shall check that corrective measures are implemented as planned and shall take appropriate actions when non-conformity with the criteria are not revolved according to the action plan.

Note: Checking that the non-conformities are solved may lead to a complementary evaluation.

7.11(2) If the certification is terminated by request of the client, the certification body shall inform the CNIL in writing and within a delay of 30 calendar days starting from the date the termination request is received.

7.11(3) When the certification is withdrawn, suspended, reinstated after suspension or when the scope of the certification is reduced, the certification body shall inform the CNIL in writing of its certification decisions according the requirements in §7.6 of this document.

7.11(4) In case the certification decision is to not grant the certification, to suspend or withdraw the certification, the client shall be informed of the options it has to appeal the decision of the certification body, of the means available to appeal this decision and of the applicable deadlines.

7.12 Records

7.12(1) In addition of the requirements in §7.12 of ISO 17065, the certification body shall retain records to demonstrate that the requirements in this document have been effectively fulfilled. As a minimum, this documentation shall:

a) include records related to the certifications that were issued and denied;

b) include records related to pending certification applications;

c) be available for a period of 6 years, including reports related to its evaluation activity (§7.4) and its surveillance activity (§7.9). In the event of disputes between the certification body and the client or in the case of an appeal to the CNIL, the retention period related to these documents for the purpose of the litigation/dispute are defined according the rules applicable to this dispute;

d) can be communicated to the CNIL, upon request, including evaluation reports (see requirements in §7.4(9) and 7.9(3) of this document). A French translation of a part of this documentation shall be communicated to the CNIL when requested.

7.13 Complaints and appeals

7.13(1) In addition to the requirements in §7.13 of ISO 17065, the certification body shall have a documented process to receive, evaluate and make decisions on complaints and appeals related to its certification process, taking into account the rules defined by the certification scheme. As a minimum, this procedure shall define:

a) who can lodge complaints and appeals;

b) who is responsible for gathering and verifying all necessary information (as far as possible) to progress complaints and appeals to a decision;

c) who is responsible for deciding the resolution of a complaint or appeal;

d) the different steps when the complainant/appellant is informed about the progress, the outcome and the end of the complaint/appeal process;

e) how verifications will take place;

f) which processes can be initiated to resolve the complaints and appeals, including the possibilities for consultation of interested parties.
7.13(2) The certification body shall confirm whether the complaint relates to certification activities for which it is responsible. This confirmation shall be given to the complainant within a delay that does not exceed one month. That period may be extended by one further month where necessary. The certification body shall inform the complainant of any such extension within one month of receipt of the request, together with the reasons for the delay.
7.13(3) The certification body shall inform the public about the procedure for the filing of a complaint or making an appeal. This procedure shall be easily accessible to data subjects concerned by the personal data processing in the scope of the certification.
7.13(4) The certification body shall inform the complainant about the progress and the outcome of this demand within reasonable time, as defined by its complaints and appeal documented process. When a formal notice of the outcome of the complaint process cannot be given, the certification body shall inform the complainant about the end of the complaint and the reasons why the outcome was not reached.
7.13(5) The certification body shall ensure that the processing of the handling of complaints and appeal is separated from its evaluation, review and certification decisions activities to ensure that there is no conflict of interest.
7.13(6) The certification body shall undertake and maintain a record of complaints and appeals. It shall include: a) the progress status of each complaint or appeal (e.g. received, under investigation, closed, etc.); b) the dates of the actions taken (e.g. complaint/appeal registered, acknowledged, progress update, final response, discontinued, etc).
8. Management system requirements
8.1 General
8.1(1) In addition to the requirements in §8 of ISO 17065, the certification body shall establish and maintain a management system that is capable of achieving the consistent fulfilment of the requirements of this document for the certification mechanisms in the scope of its accreditation. It includes that the implementation of these additional requirements shall be documented, evaluated and monitored independently to ensure compliance, transparency and verifiability with respect to the requirements of this document. To this end, the management system shall specify a methodology for achieving and controlling the implementation of these additional requirements in compliance with data protection regulations and for continuously checking them. In particular, the management system shall ensure that the requirements in §4.6 (Publicly available information) and §7.8 (Directory of certified products) of this document are achieved, so that it is made public, permanently and continuously, which certifications were carried out by the certification body, on which basis (or certification mechanisms or schemes), how long the certifications are valid and under which framework and conditions (recital 100).
8.1(2) The management principles and their documented implementation shall be disclosed by the certification body during the accreditation procedure and upon request from the CNIL at any time.
8.2 General management system documentation
8.2(1) Requirements of §8.2 of ISO 17065 shall apply.
8.3 Control of documents
8.3(1) Requirements of §8.3 of ISO 17065 shall apply.
8.4 Control of records
8.4(1) Requirements of §8.4 of ISO 17065 shall apply.
8.5 Management review

8.5(1) Requirements of §8.5 of ISO 17065 shall apply.
8.6 Internal audits
8.6(1) Requirements of §8.6 of ISO 17065 shall apply.
8.7 Corrective actions
8.7(1) Requirements of §8.7 of ISO 17065 shall apply.
8.8 Preventive actions
8.8(1) Requirements of §8.8 of ISO 17065 shall apply.
9. Further additional requirements
9.1 Continuation of the evaluation methods
9.1(1) The certification body shall establish procedures for the update of the evaluation methods that shall be applied in §7.4 of this document. In particular, this update must be considered based on changes affecting certification (see requirements in §7.10 of this document) and as preventive actions where as required in §8.8 of ISO 17065.

7. Specific application rules for certification mechanism

Application rules that are specific to a given certification mechanism and that shall be followed by the certification body for its accreditation may be defined in the scheme of the certification mechanism approved under article 42 of the GDPR.