Deliberation 2022-095 of September 22, 2022National Commission for Computing and LibertiesNature of the deliberation: Referential/standard regulation/standardLegal status: In force Date of publication on Légifrance: Sunday October 09, 2022NOR: CNIL2227754XDeliberation n° 2022-095 of September 22 2022 adopting the requirements of the accreditation reference system for certification bodies for the certification mechanisms approved under Article 42 of the General Data Protection RegulationThe National Commission for Computing and Liberties,

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general regulation on the data protection), in particular Articles 43 and 57-1-p;

Considering the law n° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms, in particular its article 8-I-2°-h;

Having regard to decree n° 2019-536 of May 29, 2019 taken for the application of law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms, in particular its article 74;

Having regard to Guidelines 1/2018 relating to certification and the definition of certification criteria in accordance with Articles 42 and 43 of Regulation (EU) 2016/679 adopted on June 4, 2019 by the European Data Protection Board;

Having regard to guidelines 4/2018 relating to the accreditation of certification bodies under Article 43 of Regulation (EU) 2016/679 adopted on December 4, 2018 by the European Data Protection Board;

Having regard to Opinion 12/2022 relating to the Commission's draft reference system concerning the accreditation of certification bodies adopted on July 4, 2022 by the European Data Protection Board under the consistency control mechanism of Articles 63 and 64 of the GDPR; On the proposal of Mrs Anne DEBET, commissioner, and after having heard the observations of Mr Benjamin TOUZANNE, government commissioner,

Makes the following observations: Article 43 of the General Data Protection Regulation (GDPR) provides that the issuance of a certification may be carried out by a body which has an appropriate level of expertise in data protection . These bodies must be approved for this purpose; Article 57-1-p of the GDPR provides that each supervisory authority drafts and publishes the requirements relating to the approval of certification bodies pursuant to Article 43; Article 64-1-c of the GDPR indicates that draft decisions aimed at approving authorization requirements established by each supervisory authority at national level are subject to the consistency control mechanism and must be communicated to the European Data Protection Board. data

(EDPS); On 27 January 2022, a draft authorization was adopted by the Commission and submitted to the EDPS on 31 January 2022. The EDPS adopted a favorable opinion on this draft on 4 July 2022, which was notified to the Commission on 11 July 2022. Adopts requirements for a reference system for the accreditation of certification bodies for certification mechanisms approved under Article 42 of the General Data Protection Regulation. This decision will be published in the Official Journal of the French Republic.ANNEXEREFERENTIAL RELATING TO THE ACCREDITATION REQUIREMENTS OF CERTIFICATION BODIES FOR CERTIFICATION MECHANISMS APPROVED UNDER ARTICLE 42 OF THE GENERAL DATA PROTECTION REGULATIONYou can consult the full text with its images from the extract from the authenticated electronic Official Journal accessible at the bottom of the page1. Who is this reference for? This reference is intended for the certifying bodies mentioned in article 8 of the Data Protection Act who wish to obtain an authorization allowing them to certify according to the criteria of a certification mechanism approved under Article 42 of the General Data Protection Regulation (GDPR).2. Scope of the standard This standard sets the requirements that the certifying body must meet in order to obtain and then maintain its approval. It constitutes the general framework applicable for certification according to the certification mechanisms approved under Article 42 of the GDPR when t has been decided, in accordance with the cooperation agreement concluded between the CNIL and the French Accreditation Committee (COFRAC), that the latter proceed with the approval of certification bodies. In this case, the accreditation issued by COFRAC takes the place of approval within the meaning of Article 43 of the GDPR. This general framework can be supplemented by application procedures specific to a certification mechanism. In this case, rules specific to the implementation of the certification mechanism specify the requirements of this reference system for the evaluation of certification bodies. This reference system is not applicable when the CNIL decides to carry out all or part of the approval of certifying bodies.3. Accreditation methods The candidate certification body submits an accreditation application file to COFRAC. This file specifies the scope of its accreditation application by indicating the certification mechanism approved under Article 42 of the GDPR for which it wishes to issue certifications. During the transitional period between submitting its file and obtaining accreditation, the certification body is authorized to begin its certification activity provided it has received a favorable response from COFRAC following the review of its application for accreditation, called operational admissibility in accordance with the COFRAC accreditation regulations. This transitional period cannot exceed 12 months: the certification body has a period of 12 months from the date of the favorable response from COFRAC to obtain accreditation. The cooperation agreement signed on May 20, 2020 between the CNIL and COFRAC sets out the roles, responsibilities and operational

procedures related to the accreditation of certification bodies for approved certification mechanisms under Article 42 of the GDPR.4. Duration of approval The duration of approval is that of the accreditation issued by COFRAC.5. Obligations of the certification body To obtain its accreditation, the certification body must: (1) Be able to demonstrate to COFRAC its compliance with the requirements defined in part 6 of this reference system; (2) Establish a procedure to investigate and respond, in writing and as soon as possible, to any request for information from the CNIL concerning the provision of aggregated data relating to the certification activity (statistics) or data relating to compliance with the requirements of this reference system , in particular for the requirements relating to the handling of complaints and appeals in connection with the certification activity. He must inform COFRAC:(3) If he is the subject, or has been the subject, of an inspection, a sanction decision and/or recent corrective measures pronounced by the CNIL or by another competent supervisory authority within the meaning of the GDPR;(4) Any other binding decision which could constitute non-compliance with this standard, including the decisions of competent judicial authorities;(5) In the event of significant changes in its status legal or any other situation affecting its activity which would be likely to call into question its compliance with this standard;(6) Other changes before their implementation when the certification mechanism introduces new rules which substantially modify the conditions of accreditation (e.g. substantial modifications relating to the evaluation methodology) or when the criteria of the certification mechanism are updated.

He must inform the CNIL:(7) Before starting to operate a European data protection seal approved by the European Data Protection Board (EDPB) in a new Member State from a satellite office. In this case, the certification body must also inform the competent control authority of this Member State. It is also subject to the following obligations:(8) In the event of suspension of the accreditation, it is no longer authorized to issue certificates until the suspension is lifted by COFRAC. During this period, the certification body must nevertheless continue to monitor valid certifications;(9) In the event of withdrawal or termination of accreditation, cessation of certification activity, or when the certification body certification was authorized to start its certification activity following the admissibility of its accreditation request but did not manage to obtain accreditation from COFRAC within the time limits, it is no longer authorized to issue certificates. Certificates already issued by the certification body remain valid for a period of 6 months. He must inform the organizations holding a certificate issued by the certification body (certified organizations) or in the process of being certified. They choose another certifying body accredited or in the process of being accredited by COFRAC to transfer their certification.6. Requirements to be met by certification bodies

Evaluation repository

GDPR Article 42 Approved Certification Mechanisms

Version of 22-09-20221. Scope This document includes requirements relating to the skills, consistency of activities and impartiality of certification bodies involved in certification mechanisms approved by the CNIL or by the European Data Protection Board (EDPS), in accordance with Article 42-5 and Article 43-2-b of the General Data Protection Regulation (GDPR).The nature of the processing of personal data within the scope of the certification mechanism ( for example, a certification applicable to processing relating to cloud services) must be taken into account during the certification body's accreditation process. For example, this includes consideration of the type of data processing operations to which the certification criteria apply, the skills appropriate for carrying out the certification activities, or the assessment methods relevant to establishing compliance with the criteria. for this purpose, a certification scheme can specify the requirements of the EN ISO/IEC 17065 standard or the requirements of this reference system, for certain fields of application of a certification mechanism. The requirements of this reference system refer to the rules which may be defined by the certification scheme and which are then binding on the certification body within the framework of its accreditation.2. Normative referencesEN ISO/IEC 17065: 2012: Conformity assessment - Requirements for bodies certifying products, processes and services ( ISO 17065 in the rest of this reference document). By default, all the clauses of the ISO 17065 standard s apply. The additional requirements defined in this reference system add specificities related to the assessment of personal data processing implemented by a data controller or a subcontractor, in accordance with Article 43-1-b of the GDPR. The GDPR takes precedence over the ISO 17065 standard. However, the additional requirements defined in this standard cannot contradict the rules concerning the organization and operation of the accreditation of assessment bodies responsible for carrying out assessment tasks. conformity defined by Regulation (EC) No. 765/2008 of the European Parliament and of the Council of July 9, 2008. If reference is made to other ISO standards in the diagram of a certification mechanism approved by the CNIL or by the EDPS, these are interpreted in accordance with the requirements defined by the GDPR.3. Terms and definitions The terms and definitions of the EDPS Guidelines on accreditation (1) and certification (2) apply. These supplement the terms and definitions of the EN ISO/IEC 17065:2012 standard. In order to facilitate the reading of this standard, the main definitions are listed below. GDPR: Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general regulation on data

protection) Data Protection Act: Act No. 78 -17 of 6 January 1978 as amended relating to data processing, files and freedoms EDPS: European Data Protection Committee CNIL: National Commission for Data Protection and Freedoms Certification mechanism: compliance tool enabling a data controller or a subcontractor to obtain certification relating to its personal data processing operationsScope of the certification mechanism: all personal data processing operations that meet the eligibility conditions of the certification mechanismCertification: attestation issued by an independent third party according to which compliance with certification criteria has been proven. Certification criteria: assessable requirements according to which the conformity assessment is carried out. The certification criteria are subject to approval by the EDPS or by the CNIL (approved criteria) Certification process: all the activities leading to the issuance of the certification and the maintenance of the validity of this certificate (e.g. .: activity of evaluation, monitoring, etc.)Audit: methodical, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which criteria are met

Note 1: internal audits are carried out by or on behalf of the organization itself.

Note 2: Second party audits are performed by parties with an interest in the organization, such as customers or others acting on their behalf. Audit plan (or assessment plan): description of the activities and provisions necessary to carry out an audit Finding (or observation): results of the evaluation of the evidence gathered during the audit, in relation to the certification criteria Evidence: recording, statements of facts or other information relevant to the criteria of certification and verifiableNon-conformity: non-satisfaction of a certification criterionAudit report (or evaluation report): document used to present the results of the auditApproval: certificate issued to a certification body, constituting recognition of its competence to apply the certification process and authorizing it to issue the certification Certification body: conformity assessment body which operates a certification mechanism by carrying out the tasks of the certification process Related body: body linked to the certification body , in whole or in part, through common shareholders, sharing the same board members, contractual arrangements, common names, common personnel, informal arrangements or other resources, such that the related body is directly concerned by any certification decision or has the ability to influence the process Accreditation requirements: requirements to be met by the certification body when implementing the certification process in order to obtain the accreditation and then keep it (subject of this standard for certification mechanisms approved under Article 42 of the GDPR) Scope of certification activities (or scope of accreditation): activities carried out by the certification body for which the -it has an accreditation Certification scheme (or certification program): set of requirements, rules and procedures applicable to a

certification mechanism. The certification scheme includes the certification criteria, certain rules relating to the application of the accreditation requirements and a set of procedures applicable to the certification process, in particular with regard to the implementation of the evaluation methodOwner of the scheme certification: person or body responsible for developing and updating the certification schemeClient (or candidate): data controller or subcontractor who has obtained certification or who has requested it from a certification bodyObject certification (or target of evaluation): set of personal data processing operations, which are involved in a product, process or service within the meaning of the ISO 17065 standard, that a data controller or a subcontractor wishes to submit to the certification process Scope of the certification: set of activities carried out by the client (or the applicant) which involve the object of the certification. Identifying the certification scope allows the certification body to determine the scope of the certification process (e.g. geographical location of activities, outsourced processing, etc.)Assessment method: procedure(s) implemented by the certification body for the evaluation of the object of certificationAppeal: request expressed by a client to a certification body to reconsider any unfavorable certification decision with regard to of the status of the certification they have requestedComplaint (or claim): any expression of dissatisfaction, other than an appeal, issued by any person or organization with a certification body, and relating to their certification activitiesTransfer of certification : recognition of an existing and valid certification, which is issued by an accredited certification body, by another accredited certification body, in order to issue its own certification(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_fr4. General requirements4.1. Legal and contractual domain4.1.1. Legal liability4.1(1) The certification organization must implement up-to-date procedures taking into account the liability regime to which it is subject in respect of its missions as provided for in the conditions of accreditation, including compliance with the requirements of this standard in accordance with article 43-1-b of the GDPR. personal data of its client as part of the certification process.4.1.2. Certification contract (between the certification body and its customers)4.1.2(1) In addition to the requirements of § 4.1.2 of ISO 17065, the certification body must ensure that the contract for the supply of The certification activities also contain client commitments on the following points: a) Comply with the certification criteria and implement the necessary changes when they are updated, in particular when these are communicated by the certification body; b) Provide the certification body with the information and access to data processing that is necessary for the execution of the certification procedure in accordance with Article 42-6 of the GDPR, within the limits

of the compliance with the organizational and technical measures implemented for this data processing in order to ensure compliance with the GDPR and the Data Protection Act.

This includes provisions for access to documentation and records, access to necessary equipment, sites or areas, exchange with its personnel and access to relevant information relating to its subcontractors; c) Take the provisions necessary to allow the participation of the CNIL and COFRAC in the evaluation of the client as an observer; d) Respect the applicable deadlines and procedures. The certification contract must mention that the deadlines and procedures deriving, for example, from the certification scheme or other regulations must be respected; e) Inform the certification body in the event of significant changes in its legal situation or its factual situation, significant changes in data processing within the scope of the certification, any change likely to affect compliance with the certification criteria or any change concerning information appearing on the official certification documentation as provided for in § 7.7 of this standard (certificate); f) inform the certification body without delay of breaches of the GDPR or the Data Protection Act when they are established by the CNIL, or by a judicial authority, and that they are likely to constitute non-compliance with the certification criteria; g) Authorize the certification body to communicate to the CNIL:

- information relating to the issue and withdrawal of certification in accordance with the requirements of §7.6 (Certification decision) of this reference system;
- at the request of the CNIL, information relating to the certification procedure in accordance with the requirements of §7.12 (Records) of this standard.4.1.2(2) The contract for the supply of certification activities must also inform the client of the points following: a) The certification does not reduce the responsibility of its client in terms of compliance with the provisions of the GDPR and the Data Protection Act and is without prejudice to the exercise of the missions and powers of the CNIL provided for in particular in Articles 20 to 23 of the Data Protection Act; b) The evaluation methods that will be applied by the certification body for the examination of the target of evaluation, as provided for by the requirement in §7.3(2) b ) of this standard; c) Organizational measures and procedures put in place by the certification body for the purpose of managing complaints and appeals, in accordance with article 43-2-d of the GDPR. The certification body must also ensure that the contract commits the client to comply with the rules provided for by these procedures with regard to the investigation of complaints provided for in §4.2.2.2 of the ISO 17065 standard; d) Rules applicable to the maintenance of the certification, its renewal, its suspension and its withdrawal, in accordance with article 42-7 of the GDPR, including the rules relating to the intervals for monitoring and

reassessment of the certification in accordance with the requirements of § 7.9 of these standards; e) The general consequences of the end of the accreditation period, suspension, withdrawal or non-issuance thereof. The actions available to the customer to maintain the validity of the certification or renew it are also specified. In particular, the certification body informs the customer of the general conditions applicable to the transfer of a certification and of the procedure applicable in the event that it is the subject of a decision to refuse, suspend or withdraw its approval for a certification mechanism approved under Article 42.

4.1.3. Use of licenses, certificates and marks of conformity4.1.3(1) In addition to the requirements of §4.1.3 of ISO 17065, the certification body must exercise control over the use and display of licenses , certificates and conformity marks, as well as any other device intended to identify a certified product, process or service, ensuring that: a) The certification mechanism is clearly mentioned and, when applicable, the subset of criteria applicable to the TOE is indicated. In particular, the communication is transparent on the type of processing operations covered by the certification criteria when the certification mechanism applies to a specific domain; b) The scope of the certification is unambiguous in order to prevent any confusion concerning the data processing that has been evaluated; c) The rules for the use of trademarks registered by the CNIL for certified organizations are respected. Note: In the case of a general certification mechanism, it is possible that only a sub -set of criteria applies to certain TOEs. For example, when the scope of the certification mechanism allows both controllers and processors to apply, the list of criteria that will apply to the target of evaluation of a controller treatment will be significantly different from the list of criteria that will apply when the processing operations of the personal data of the target of evaluation are carried out by a processor on behalf of a data controller.4.1.3( 2) The incorrect or ambiguous use of licenses, certificates, marks of conformity, as well as any other device intended to identify a product, a process or a certified service must be corrected by an appropriate action. At a minimum, this includes: a) The obligation for the certified to take measures to put an end to incorrect or ambiguous practices; b) The obligation for the certified to renew the information of the public, by default, using means communication methods similar to those used previously; c) Informing the CNIL, as soon as possible, of the non-compliant practices observed and the actions taken by the certification body and the client; Note: Other appropriate actions decided by the certification body may also include the withdrawal or suspension of certification, a communication relating to the fault committed or, if necessary, the exercise of an action before the competent courts.4.2. Management of impartiality4.2(1) In addition to the requirements of §4.2 of ISO 17065, the certification body must provide evidence: a) Of its independence in accordance with article 43-2-a of

the GDPR . This includes evidence regarding the funding of the certification body as far as the assurance of impartiality is concerned; b) That its tasks and obligations do not give rise to a conflict of interest within the meaning of Article 43 -2-e) of the GDPR; c) That he has no significant relationship with the clients he assesses. Note: In addition to the requirements of this reference system aimed at preventing conflicts of interest, the requirements of § 4.2 and §5.2 of ISO 17065, concerning the management of identified conflicts of interest, apply. In particular, the certification body must regularly identify the risks likely to affect its impartiality and must take the necessary measures when it becomes aware that its impartiality is threatened by the actions of other persons, entities or bodies.4.2(2 ) In particular, the certification body must ensure for each of its clients that: a) The personnel involved in the certification assessment, review and decision-making procedures have no other link with its client than its certification activity and has no activity related to the subject of the certification which would be likely to call into question 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) which poses a risk to the impartiality of the certification body; c) It has not had any economic relationship with its client since at least 2 years (with the exception of those defined by a certification contract) and is not financed by its client for activities other than certification. In particular, the certification body must not entrust personal data processing activities to its client.4.3. Liability and financing4.3(1) In addition to the requirements of §4.3 of ISO 17065, the certification body must take the necessary measures (for example, insurance or provisions) to cover its commitments in the geographical regions where it operates the certification mechanism.4.4. Non-discriminatory conditions4.4(1) In addition to the requirements of §4.4 of ISO 17065, the certification body must be transparent with the applicants concerning: a) The types of data processing which are the scope of the certification mechanism and which are also within the scope of its certification activities (scope of accreditation).

In particular, when the certification body does not have an adequate assessment methodology for the assessment of data processing for a sector of activity (for example, when the assessment involves the processing of particular categories of data personal nature or the use of sector-specific technologies) or when its personnel do not have the appropriate skills to assess a type of data processing, the certification body informs applicants of these limitations and provides a list of sectors of activity in the scope of its evaluation activities for this certification mechanism; b) The list of Member States of the European Union which are in the scope of its certification activities, for a transnational certification mechanism approved by several competent supervisory authorities or for a European data protection seal approved by the EDPS. In particular, when the certification body

does not have an adequate evaluation methodology for the evaluation of data processing subject to the national specificities of a law relating to data protection of a Member State of the European Union or when its staff does not have the appropriate skills to assess the processing operations in the context of the national specificities of a Member State, the certification body informs the candidates of these limitations and provides a list of the Member States of the European Union within the scope of its evaluation activities for this certification mechanism.4.5. Confidentiality4.5(1) In addition to the requirements of §4.5 of ISO 17065, the certification body must inform the client of the information that will be provided to the CNIL for the purposes of implementing the certification process. This includes the following information: a) Certification decisions (see the requirements of §7.6 of this standard); b) The information to be submitted to the CNIL as part of the directory of certified persons (see the requirements of §7.8 of the this standard).4.5(2) The certification body must inform the client that, at the request of the CNIL, it may be required to send it additional information in connection with its assessment in order to demonstrate the conformity of the certification process. certification to the requirements of this standard (see requirements of §7.12 of this standard), including information protected by contractual confidentiality which is linked to compliance with data protection rules. In particular, the certification body must not not collect confidential information for which the client could legitimately invoke the secrets opposable to the members and agents of the CNIL in the exercise of their missions and strictly delimited in article 19-III of the Data Protection Act, namely: information covered by the professional secrecy applicable to relations between a lawyer and his client, by the secrecy of the sources of journalistic processing or by medical secrecy.4.5(3) The certification body must inform the client that the CNIL has the power to carry out a review of the certifications issued pursuant to Article 42-7 of the GDPR. The conditions applicable to the exercise of this power conferred on the CNIL by virtue of Article 58 are defined by the GDPR and the Data Protection Act and are outside the scope of this reference system.4.6. Publicly available information4.6(1) In addition to the requirements of §4.6 of ISO 17065, the certification body shall make available to the public: a) All versions (current and previous) of the certification criteria which are currently used in the certificates issued, mentioning their respective validity periods; b) Obsolete versions of the certification criteria which are no longer used in valid certificates, mentioning their respective validity periods; c) Updated certification procedures, including including the procedures for handling complaints and appeals in accordance with Article 43-2-d of the GDPR; d) Information on how the certification procedures are implemented in practice, in particular on the means made available to persons concerned by the processing of personal data within the scope of the certification to make a complaint and on the way in which it will be treated by the certification body.5. Structural

requirements5.1. Organization and management5.1(1) The requirements of §5.1 of ISO 17065 apply.5.2. Mechanism for preserving impartiality5.2(1) The requirements of §5.2 of ISO 17065 apply.6. Resource Requirements6.1. Certification body staff6.1(1) In addition to the requirements of §6.1 of ISO 17065, the certification body must establish, implement and maintain a competency management procedure in order to demonstrate that its staff has the appropriate and up-to-date skills (knowledge and experience), in accordance with Article 43-1 of the GDPR, to carry out its certification activities. In particular, staff must: a) Have received specific training in the protection of personal data; b) Have relevant and appropriate knowledge and experience in terms of analysis and/or implementation of the regulations applicable to the protection of personal data (GDPR, the Data Protection Act and other national laws applicable to data processing within the scope of the certification mechanism); c) Have the knowledge and relevant and appropriate experience in the analysis and/or implementation of technical and organizational data protection measures within the scope of the certification mechanism, in accordance with Article 43-2-a of the GDPR; ) Have appropriate experience in the evaluation of data processing (audit). Note: The 'relevant' and 'appropriate' character of the knowledge and experience of the personnel must be defined by the certification body in such a way that each person involved in the certification process (application processing, evaluation, review, decision-making, monitoring, etc.) is able to carry out its tasks, taking into account the rules defined by the certification scheme and in compliance with the minimum requirements defined by this reference system with regard to the skills of the personnel. This includes taking into account specific skills needs related to the scope of the certification mechanism and/or the assessment targets that may be offered for certification, for example, for particular sectors of activity to which the certification mechanism applies (eg: data hosting), certain categories of personal data (eg: health data) or even specific technologies implemented by certain services (eg. ex. : internet tracking technology).6.1(2) The certification body must ensure that the personnel in charge of assessments have: audit technique, audit documentation, audit rules and requirements, etc.); b) Participated in at least 2 complete audits, from the preparation of the audit to the final conclusions, over the last 3 years.Note: Internal audits and second party audits are accepted when the assessment has been carried out on the basis of requirements or established internal rules and according to an audit procedure.6.1( 3) The certification body must ensure that the personnel responsible for the review and/or certification decision-making have in-depth knowledge and experience of: a) State of the art, risks and issues relating to the protection of personal data; b) Implementation of the certification process. Note: When the certification body appoints a person or a group of persons to make a certification decision in accordance with §7.6.2 of ISO 17065 and if this

staff does not have the knowledge or experience required in 6.1(3) of this standard, the certification process leading to this individual certification decision must include a certification review process which involves at least one person with the skills required by the requirement in §6.1(3) of this standard.6.1(4) The certification body must have staff with technical expertise and legal expertise whose profiles meet:a ) The requirements relating to the technical expertise profile, as defined in §6.1(5), §6.1(6) and §6.1(7) of this standard; b) The requirements relating to the legal expertise profile, such as defined in §6.1(8) and §6.1(9) of these standards. Note: Internship and apprenticeship periods do not constitute work experience taken into account to certify the number of years of professional experience required for the staff responsible for the assessment or review of the certification, as set out in these standards.6.1(5) (Profile of technical expertise) The certification body must ensure that the staff with a technical expertise justifies: a) At least a bachelor's degree, or corresponding at least to level EQF6 (3) of the European qualifications framework, in the field of IT, information systems or cybersecurity or property of a title recognized by the State (p. ex. : engineering degree) in these fields;b) Or has significant professional experience of at least 5 years in the field of data protection.Note: The professional experience required in §6.1(5) b) of this standard constitutes an alternative to the diploma required in §6.1(5) a) (Validation of Acquired Experience - VAE in the context of this standard). This same professional experience may also be taken into account, when appropriate, to meet the other professional experience requirements of this standard.6.1(6) (Technical expertise profile) The certification body must ensure that its personnel with technical expertise have undergone training of at least 2 days on the useful reference systems for managing the security of information systems (regulations, standards, methods, good practices, risk management, etc.) .).6.1(7) (Technical expertise profile) The certification body must ensure that its staff with the technical expertise profile have appropriate and up-to-date skills which include: evaluation, a minimum of 2 years' experience in the field of data protection, such as the analysis and/or the implementation of technical and organizational measures for securing information systems and which is adapted to the field of application of the certification mechanism (p. ex. : tests of data security measures, evaluation procedures or technical certifications); identification, definition, monitoring of data protection measures or in a data protection advisory activity.6.1(8) (Legal expertise profile) The certification body must ensure that its personnel legal expertise justifies: a) At least a master's degree 1 in the field of law or a diploma recognized by a Member State of the European Union, corresponding to at least 8 semesters and leading to an equivalent university degree (master's degree in law);b) or has 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 standard constitutes an

alternative to the diploma required in §6.1(8) a) (Validation of Acquired Experience - VAE in the context of this standard). This same professional experience may also be taken into account, when appropriate, to meet the other professional experience requirements of this standard.6.1(9) (Legal expertise profile) The certification body must ensure that its staff with a legal expertise profile has appropriate and up-to-date skills which include: a) For the staff in charge of the evaluation, a minimum of 2 years' experience in the field of data protection law, such as the analysis and/or the implementation of compliance with the regulations applicable to the processing of personal data (e.g.: review of contracts or assessment procedure relating to the rights of the persons concerned); b) For the personnel responsible for reviewing the certification (or decision-making), at least 2 years' experience in monitoring the compliance of data protection measures or in an advisory activity in the field of personal data protection staff.6.1(10) The certification body must ensure that the skills of its staff are maintained, for example by means of a professional training programme.6.1(11) In addition to the requirements of §6.1.3 of the ISO 17065, the certification body must require its personnel participating in the certification process to undertake to respect the rules defined by the certification body with regard to the independence of personnel with commercial or other concerning the object of certification in accordance with article 43-2-a of the GDPR. The certification body must use this information as input data to identify the risks posed to impartiality by the activities of this staff or organizations that employ them in accordance with the requirements of §4.2.3 of ISO 17065 and demonstrate that their missions do not lead to a conflict of interest in accordance with article 43-2-e of the GDPR.6.2. Resources for assessment6.2(1) In addition to the requirements of §6.2 of ISO 17065, the certification body must ensure that the organizations to which assessment activities are outsourced, and the personnel to whom those they use to carry out these activities, meet the requirements of this reference system which apply to the assessment activity. In accordance with the requirements of §6.2.2.4 and §7.6.1 of ISO 17065, the organization certification body shall take full responsibility for all activities outsourced to another body and it shall be accountable and shall retain its decision-making power in matters of certification.6.2(2) In particular, when assessment activities are outsourced with another organization, the certification body must: a) Check, for each person in charge of the assessment, that the requirements of §6.1 of this reference system are met; b) Check that the personnel involved in the process of certification has no other link of interest with the client than the certification process and has no activity related to the client's activity which would be likely to call into question the impartiality of the certification body (see requirements of §4.2 of this reference system).7. Process requirements7.1.General7.1(1) The requirements of §7.1 of ISO 17065 apply.Personal data processing operations must be

assessed according to the certification criteria approved by the CNIL under article 58-3 of the GDPR and article 8-I-2°-h of the Data Protection Act or by the EDPS under Article 63 of the GDPR.Note: To carry out its assessment, the certification body may take into account the guides as well as the assessment or test methods provided by the owner of the certification scheme .7.2. Application7.2(1) In addition to the requirements of §7.2 of ISO 17065, the certification body must collect the following information from the candidate in relation to the object of certification: a) A detailed description of the target assessment, including its interfaces with other systems and/or organizations. In particular, the underlying protocols and guarantees related to these exchange interfaces, which allow the communication of data between the target of evaluation and external systems and/or third-party organizations, are provided; b) The list of transfers of data to organizations located in a third country (outside the European Union) or to an international organization. The national regulations applicable to the data importer and the type of appropriate guarantees implemented are indicated; c) The responsibilities, processing activities and/or role of the candidate, when the candidate is a processor or a data controller spouse; d) The list of subcontractors (or subsequent subcontractors when the candidate is himself a subcontractor). Their responsibilities and their processing activities must be described and the main contracts or standard contracts linking the applicant to its subcontractors must be identified; e) The list of joint data controllers. Their responsibilities and roles are described and the principles of the agreement binding them with the candidate must be indicated (or the nature of the legal instrument used); f) The general characteristics of the data processing within the scope of the certification, such as the address of the candidate's premises where the personal data is processed, the categories of data involved and the national obligations that apply to the data processing; g) Where applicable, information relating to certifications or results evaluations obtained before the application for certification, when the nature of these evaluations and their scope are relevant for possible consideration in the certification process; h) The existence of any control action in progress, or sanction decision and/or recent corrective measures pronounced by the CNIL or by another competent supervisory authority against the candidate, when it relates to data processing within the scope of the certification requested.7.3 Review of the application7.3 (1) To examine certification applications according to the requirements of §7.3 of ISO 17065, the certification body must take into account the information obtained in §7.2 of this standard.7.3(2) In addition to the requirements of § 7.3.1 of ISO 17065, the certification body must carry out a review of the information obtained in order to guarantee: a) That the object of certification is eligible for assessment according to the certification criteria, taking into account the rules defined by the certification scheme. In particular, the certification body must ensure that the candidate and the data

processing operations it wishes to submit for assessment are within the scope of the certification mechanism with regard to:

- the candidate's responsibilities for the proposed object of certification, taking into account the applicable data protection regulations (data controller, joint data controller, subcontractor, subsequent subcontractor, etc.);

- the type of data processing operations of the object of certification, taking into account the data processing operations for which the certification criteria have been designed and approved under Article 42 of the GDPR; b) That it has evaluation methods adapted to the target of evaluation, taking into account:

- the rules defined by the certification scheme concerning the methods to be applied for the assessment of the compliance of data processing operations with the certification criteria;

- the regulations applicable to the target of evaluation in terms of data protection;

- the control actions in progress or the decisions of sanction and/or recent corrective measures pronounced by the CNIL or other competent control authorities. The certification body describes the evaluation methods used for the conformity assessment of the processing operations to the certification criteria in a uniform manner, ensuring that comparable evaluation methods are used for the evaluation of comparable evaluation targets and conclude with comparable results; c) That he has the legal skills and techniques necessary in terms of data protection, in accordance with the requirements of §6 of this standard, to carry out the certification activity, in particular when the certification body does not have subsequent experience of evaluating the same type of object of certification or a similar scope of certification.7.3(3) When the certification scheme defines rules for calculating the duration of the assessment activity (p. ex. : in days), the certification body must set up a procedure for calculating the duration of the audit. For the application of the evaluation method, this procedure must take into account the following factors: a) The extent of the processing of personal data within the scope of certification; b) The nature of the personal data processed; c) The risks for the persons concerned by the data processing; d) The complexity of the evaluation of the technologies used for the data processing; e) The use of subcontractors to carry out the data processing; number of structures/establishments of the candidate in which the processing of personal data is carried out. this calculation according to the rules defined by the certification scheme and determine if the calculated duration is sufficient to carry out its assessment tasks or if this duration must be increased. It keeps the justification and a record of the duration chosen. The duration of the audit chosen by the certification body is indicated in the certification contract. certification body in requesting the transfer of its certification, the certification body follows the rules defined by the certification scheme that apply. In particular,

the certification body must: a) Check that the candidate has a certificate valid at the time of application; b) In addition to the information listed in §7.2 of this reference system, obtain from the candidate:

- a copy of the certificate issued;

- the last audit report;

- the complaints received; c) In addition to the review provided for in §7.3(2) of this reference system, examine, by means of a documentary review, the status of pending non-conformities, the findings of the last audit report, the complaints received and the corrective actions implemented; d) Take its decision concerning the transfer of the certification within one month. Note: In the absence of receipt of all or part of the documents listed above or in case of doubt on compliance of the target of evaluation with the certification criteria, the certification body will not be able to transfer the certification as is and will have to start a new certification process starting with an initial audit, as provided for in § 7.4 of this standard.7.4. Assessment7.4(1) In addition to the requirements of §7.4 of ISO 17065, the certification body must have an assessment plan (audit plan). The audit plan must enable the implementation of the assessment method established in the certification contract, in accordance with requirement §4.1.2(2) b) of this standard. assessment may require an assessment at the customer's premises to make the findings necessary to establish compliance with the certification criteria. Any deviation from the assessment method must be justified by the certification body.7.4(2) The certification body must apply the assessment methods established in the certification contract during its assessment, for example by applying: a) A method for assessing the necessity and proportionality of data processing operations with regard to the objective pursued and the safeguarding of the fundamental rights and interests of the data subject; b) A method for assessment of the extent, type and assessment of all the risks envisaged by the controller and the processor with regard to their obligations in accordance with Articles 30, 32, 35 and 36 of the GDPR, and of the appropriateness of the technical and organizational measures provided for in Articles 24, 25 and 32 of the GDPR, insofar as the aforementioned articles apply to the subject of the certification; c) A method for the evaluation of the corrective actions, including safeguards, safeguards and procedures to ensure the protection of personal data for the data processing involved in the TOE. carry out the assessment tasks, taking into account the rules defined by the certification scheme. The certification body ensures that the personnel involved in the certification assessment tasks, whether these resources are internal to the organization or external, meet the skill requirements, as specified in §6 of these standards. In particular, for each assessment, the certification body ensures that the team in charge of the assessment, as a whole, has the legal and technical skills as

defined in §6 of these standards. Exceptionally, when the certification body involves in evaluation a person who cannot prove skills meeting the qualification requirements as a technical profile or a legal profile, as defined in §6 of this reference system, it justifies the particular need for the intervention of an expert with specific skills to carry out the assessment (e.g.: a person specialized in a particular technology, in a sector of activity involving the processing of particular categories of data or for which national regulations are applicable ). In this case, the result of the evaluation tasks carried out by the person with an expert profile must be supervised, during the evaluation process, by a staff member in charge of the evaluation and who meets the qualification requirements as a technical profile or a legal profile (e.g. the audit team leader).7.4(4) In addition to the requirements of §7.4.5 of ISO 17065 and in the As part of the application review process in §7.3 of ISO 17065, when the certification body relies on the result of a certification obtained before its assessment, the certification body must: a) Ensure that the certificate will be valid at the time of the evaluation and that the certification obtained is relevant for the target of evaluation; b) Document how and to what extent the results of the certification previously obtained can be taken into account for the evaluation of the certification criteria, in compliance with the rules defined by the certification scheme; c) Establish the consequences for the assessment still to be carried out and on the assessment method to be applied, for example by defining a correspondence matrix between the criteria of the two certification mechanisms for the TOE context. ensure compliance of the target of evaluation with all the criteria of the approved certification mechanism. In particular, the certification body must: a) Have access to the entire evaluation report of the certification previously obtained (and not only the certificate of conformity or a similar certificate); b) Document its own findings by:

- referring to the relevant results of the pre-existing evaluation report (the reproduction of the findings in the evaluation report is not required);
- making its own findings when they are necessary for the assessment of the additional criteria of the approved certification mechanism. If deviations from the findings of the assessment report of the certification previously obtained are identified by the certification body during its evaluation of the criteria of the approved certification mechanism, the evaluation is extended to the certification criteria concerned and, if necessary, for the entire target of evaluation already certified.7.4(6) In addition to the requirements of §7.4.6 of ISO 17065, the certification body must define in its procedures the way in which the client is informed of the results of the assessment, including non-conformities, taking into account the rules defined by the certification scheme, particularly with regard to the form of this information and the time when it is provided to the client.7.4(7) In addition to the

requirements of §7.4.9 of ISO 17065, the certification body must document its findings, to each certification criterion, in accordance with the rules defined by the certification scheme. At a minimum, the evaluation report includes: 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 examined ;d) References to the processing of personal data which have been assessed; e) The function of the persons who were the subject of the interview; description of the non-conformities which identifies the certification criteria which are not met and which assesses the severity and scope of the non-conformities. The certification body asks its client to propose the implementation of measures aimed at correct all non-conformities so that they can be taken into account by the certification body when making its certification decision (see requirement in §7.6 of ISO 17065). The action plan resulting from the certification decision is also appended to the assessment report. This action plan is examined by the certification body before the review and the certification decision.7.4(8) The certification body provides the CNIL, at its request, with the report of its assessments as well as its appendices. Note: to demonstrate compliance with the requirements of this standard, the certification body is not required to keep the evidence (e.g.: documents, screenshots, log files, etc.) .) which enabled it to establish the findings documented in its evaluation report.

Note: In accordance with the requirements of §7.12 of this standard, the certification body retains the report of its assessments for a period of 6 years.7.4(9) If the personal data of the scope of certification are processed from several structures/establishment of the candidate, the assessment must be carried out according to the rules defined by the certification scheme. When non-compliance is detected for one of these structures/establishments, the certification body asks its client to:

- that it analyzes its extent and causes; And
- that it proposes the implementation of measures aimed at preventing this non-conformity from recurring in other locations.

These analyzes are attached to the action plan and examined by the certification body. 7.5. Review of the results relating to the assessment7.5(1) In accordance with the requirements of §7.5 of ISO 17065, the certification body carries out a review of all the information and all the results following the assessment.In addition of the requirements of §7.5 of ISO 17065, the assessment review process must take into account the rules defined by the certification scheme. In particular, the certification body must: a) Check that the scope of the certification is consistent with the object of the certification which has been assessed; b) Check that the assessment methods have been followed and that the findings available in the assessment report

are relevant.7.5(2) The certification body shall designate personnel with appropriate skills to carry out the certification review, taking into account the rules defined by the certification scheme. The certification body ensures that the personnel involved in the certification review, whether these resources are internal to the organization or external, meet the skills requirements, as specified in §6 of these standards. In particular, for each review, the certification body ensures that the staff responsible for reviewing the assessment has the legal and technical skills as defined in §6 of these standards.7.6. Certification decision7.6(1) In addition to the requirements of §7.6 of ISO 17065, the certification body defines procedures for making certification decisions or refusing certification, taking into account the rules defined by the scheme certification body. The certification body also defines procedures for making other decisions relating to certification occurring following an assessment carried out as part of the monitoring process provided for in §7.9.2 of ISO 17065 or when the measures appropriate in response to non-compliance include an assessment in accordance with §7.11.2 of ISO 17065: renewal, updating of the scope of certification (extension or reduction of the scope), suspension or lifting of a suspension and withdrawal of certification. These procedures must provide that: a) The reasons which led to a favorable decision are identified and documented based on evidence and objective facts; b) The reasons which led to the refusal, suspension or withdrawal of certification are identified and documented, in particular with regard to the seriousness, number and recurrence of the non-conformities noted; c) The period between the end of the assessment (last findings) and the decision cannot exceed 3 months, except in exceptional circumstances for which the justifications are documented; of a control action in progress, or of a decision of sanction and/or recent corrective measures pronounced by the CNIL or other competent control authorities, the certification body checks with the client that this information is up to date. day before making a decision.

If new checks have been carried out with the client or if corrective measures have been requested, the certification body assesses whether this may constitute non-compliance with the certification criteria and prevent the certification from being issued (or renewed, reinstated or extended).

The certification body documents in its assessment report (and/or in its certification decision) its conclusions concerning the control actions or the corrective measures requested relating to the processing of data within the scope of the certification; e) L The certification body informs the CNIL of its decisions, in writing and before the application of its decision, when the certification is issued (renewed, restored or extended) or withdrawn (reduced or suspended) in accordance with article 43-5 of the GDPR;

The information provided to the CNIL must include:

- the customer's name;

- the scope of the certification;

- the description of the object of the certification;

- a summary of the evaluation report which explains how the certification criteria are satisfied (or why they are no longer satisfied);

- the official certification documentation, as provided for in §7.7 of this standard (the certificate issued); f) The certification body informs the client of the certification decisions.7.6(2) The certification body must define its procedures in order to guarantee its independence and assume its responsibilities through its certification decisions. In particular, the certification body must demonstrate that the person(s) it appoints to render a certification decision have not been directly or indirectly involved in the evaluation process.7.7. Certification document7.7(1) In addition to the requirements of §7.7 of ISO 17065, the certification body must provide the client with official certification documents (certificate) which identify: a) The name and reference (including version) of the certification criteria that were used for the assessment; b) The scope of the certification, which includes a clear and understandable description of the object of the certification and the list of customer locations where personal data is processed;

When the applicability of a subset of the certification criteria depends on the context of the processing operations within the scope of certification (e.g. the status of controller or processor, the processing of specific categories of data, the use of specific technologies, the application of specific sectors of activity, etc.), the scope of the certification must be described in such a way that the subset of the criteria that have been assessed are understandable;c ) The subject of certification (the TOE), including the version or other applicable identifiers. 7.7(2) The certification body provides its client with official certification documentation (certificate) where the expiry or expiry date of the certification is fixed in accordance with the validity period of the certification defined by the certification scheme. The certification body ensures that the period of validity of the certification does not exceed 3 years.7.8. Directories of certified products7.8(1) In addition to the requirements of §7.8 of ISO 17065, the certification body maintains up-to-date information on the certified evaluation targets, in accordance with the rules defined by the certification scheme, including at least: a) The scope of the certification; b) A clear and understandable description of the subject of the certification (a relevant description of the target of evaluation), including the version or other applicable

identifiers; c) The name and/or a reference (including the version) of the certification criteria that were used for the evaluation; d) The validity status of the certification: in progress (not yet issued), issued (certification initial), renewed, expired, terminated, suspended or withdrawn;

e) The date on which the certification was issued (or renewed); f) The dates on which the surveillance activities were carried out; g) The date on which the certification expired or expired, or the date on which the certification has been terminated, suspended, or withdrawn. Note: This information includes a history of actions taken by the certification body for each certified TOE. They do not have to be made public, unless the certification scheme stipulates that they must be published, unlike the information provided for in requirement 7.8(2) of this standard which aims to make the list of endpoints that have a valid certificate. They must nevertheless be accessible on request from a third party who wishes to be sure of the validity status of a given certification, for example, for a specific previous period or for a target of evaluation which has undergone changes during the time.Note: In accordance with the requirements of §7.12 of this reference system, the certification body keeps the records relating to the certified objects for a period of 6 years.7.8(2) The certification body must make available to the public a summary documentation of its certification decision in a way that promotes transparency regarding what was assessed and the assessment methods used. The information to be published is defined by the certification scheme. The certification body must, at the very least, publish a summary in a directory which includes: a) The name of the client and the information enabling him to be contacted; of the certification, which includes a clear and understandable description of the subject of the certification; c) The subject of the certification (the target of evaluation), including the version or other identifiers applicable; d) The name and/or a reference (including the version) of the certification criteria which were used for the assessment and, where applicable, the specifics of the method applied to assess the compliance of the data processing operations with the certification criteria; e) The date on which the certification was issued (or renewed); f) The state of validity of the certification resulting from the last certification decision. certification (in accordance with the requirements of §7.6 of this standard), the certification body provides it with this information, which will be published. The scope of the certification and the object of the certification must be provided to the CNIL in French.7.9. Monitoring and renewal7.9(1) The certification body must define a procedure for monitoring the compliance of the certified evaluation targets with the certification criteria, in accordance with article 43-2-c of the GDPR.In addition to the requirements of §7.9 of ISO 17065, the monitoring must include: a) An assessment of the changes that have been applied to the data processing concerned by the scope of the certification since the previous assessment and

their potential impact on compliance with the certification criteria b) An assessment of the certification criteria whose implementation methods were assessed during the previous audit but for which the actual implementation was not applicable, for example due to the fact that certain data processing operations had not been not yet started;c) Evaluation of the implementation of measures provided for in the action plan resulting from the previous certification decision (see the requirements of §7.4 and §7.11 of this reference system);d) An in-depth evaluation certification criteria selected from the risks of non-compliance observed during previous assessments (but which have not been the subject of a finding of non-compliance). For example, an assessment can be deepened by:

- the analysis of larger quantities of evidence (eg: files, contracts, interviews, etc.) in order to consolidate the findings already established;
- the analysis of recent recordings in order to ensure that the findings established remain valid over time, for example an assessment of compliance with the certification criteria of one or more new processing operations within the scope of the certification since the previous assessment;
- the analysis of data processing in different contexts within the scope of the certification (e.g.: evaluation in other client locations, of certain personalized services or processes, etc.) in order to ensure that the findings established are consistent.7.9(2) The certification body must plan its surveillance activity according to the rules defined by the certification scheme. The maximum period between surveillance measures should not exceed 12 months. In addition to these regular assessments, the surveillance measures necessary to maintain the certification must allow: a) To ensure that the information relating to the certification is up to date (e.g. description of the target of evaluation, etc.); b) The organization of an additional evaluation at the initiative of the certification body, when this is proportionate to the risk in terms of the protection of personal data. For example, an additional assessment may take place when non-compliance is suspected due to one or more complaints received by the certification body or information relating to non-compliant practices which have been made public or even when this is necessary to provide the CNIL with the requested information relating to compliance with the approval requirements of this standard.7.9(3) The certification body must document the results of its monitoring activity for each certification, including its consequences when the surveillance leads to a decision to reduce the scope of certification, or to suspend or withdraw the certification. Note: In accordance with the requirements of §7.12 of this standard, the certification body keeps records relating to its surveillance activity during a period of 6 years.7.9(4) When the client's request relates to the

renewal of the certification, the certification body must follow a certification process that complies with the same requirements of this standard as those applicable to a certification request initial. The certification body must follow the specific rules defined by the certification scheme which apply to the renewal of the certification. In particular, these rules may relate to the issue of the certificate (e.g. effective date of renewal of certification).7.9(5) When the client has several structures/establishments, the certification body must follow the rules applicable defined by the certification scheme, in particular with regard to the consequences on the certification process of the addition (extension of the scope) or the termination of location (reduction of the scope). In particular, the certification body plans the evaluation of the client's sites over the validity period of the certification.7.10. Changes affecting certification7.10(1) In addition to the requirements of §7.10 of ISO 17065, changes to be considered by the certification body shall include: a) Any breach of the GDPR or the law Informatique et Libertés reported by the client to the certification body when it is related to the subject of the certification; b) Any change in the processing of personal data indicated by the client as being likely to have effects on the compliance of the object of certification with the certification criteria; c) Any modification made to the regulations relating to the protection of personal data when it concerns the scope of the certification mechanism; d) The the adoption of delegated acts by the European Commission in accordance with Article 43-8 and 43-9 of the GDPR in relation to the scope of the certification mechanism; e) Binding decisions or opinions of the EDPS and/or the CNIL in connection with the scope of the certification mechanism; f) The court decisions on the protection of personal data brought to its attention in connection with the scope of the certification mechanism; g) The new state-of-the-art developments in the technologies used for the processing of personal data;

h) Emerging data protection risks. Note: The certification body may also take into account the recommendations, good practices and other documents adopted by the EDPS and/or the CNIL in connection with the scope of the certification mechanism.7.10(2) The certification body must define a management procedure allowing it to analyze, decide on and implement changes having consequences on the certification process, taking into account the rules defined by the certification scheme. At a minimum, this procedure includes the following points: a) Establishing and updating a register listing the changes analyzed as having consequences on the certification process as well as the impacted evaluation targets;

b) Document the measures decided to implement the changes having consequences on the certification, in particular:

- the additional assessment or the immediate reassessment of the certification criteria;
- the reasons which led to not immediately carrying out an additional evaluation or a re-evaluation of the certification criteria for

the impacted evaluation targets;

- the reasons which led to no evaluation being carried out and, where applicable, the other types of action implemented;

- the rules applicable to the transition periods, including when they are defined by the owner of the certification scheme when updating the certification criteria, the deadlines applicable to the changes to be implemented and the conditions to maintain or renew certification for impacted TOEs; c) Notify the client, in a timely manner, when changes affecting their certification will require assessment and what will need to be assessed (and how ) to ensure that the processing of data within the scope of the certification remains in compliance with the certification criteria. The planned evaluation must be proportionate to the consequences on the certification. When a transition period is defined, the client is informed of the deadlines to be met in order to maintain or renew their certification, as well as the consequences in the event of non-compliance; d) Revise the official certification documents (certificates) , suspend or withdraw the certification, if the assessment concludes that the data processing within the scope of the certification no longer complies with the certification criteria; e) Update its certification procedures, including the impacted assessment methods taking into account the rules defined by the certification scheme, so that they apply to future clients in a uniform manner.7.10(3) In the event that the client informs the certification body of an action of control in progress, or of a decision of sanction and/or recent corrective measures pronounced by the CNIL or another control authority, which calls into question the conformity of the customer with the rules of protection of personal data, the certification body documents the outcome of its analysis of whether the TOE remains in compliance with the certification criteria, including its consequences when the evaluation results in a certification decision.7.11. Termination, suspension or withdrawal of certification7.11(1) In addition to the requirements of §7.11 of ISO 17065, the certification body must define a procedure for managing non-conformities of the target of evaluation according to the rules defined by the certification scheme. At a minimum, this procedure includes the following points: a) When non-compliance with the certification criteria is confirmed, the certification body must determine whether the corrective actions proposed by the client are likely to remove the non-compliance before the certification decision making. This opinion is without prejudice to the conclusions of the evaluation of the implementation of the measures by the customers when it will be carried out by the certification body;

For all non-conformities, the certification body assesses whether the action plan makes it possible to guarantee the compliance of the processing operations when the certification decision is taken. If the action plan is not sufficient to guarantee it, the certification body must wait for evidence of implementation of the corrective actions to issue the certification; b) The

certification body sets a deadline for implementation corrective actions according to the level of seriousness of the non-conformities; c) When the client's certification is conditional on the implementation of an action plan, the certification body checks that the implementation of the measures aimed at to correct the non-conformities is carried out according to the planned schedule and takes the appropriate actions when the non-conformities are not resolved according to the action plan. an additional assessment.7.11(2) When the certification is terminated at the request of the client, the certification body informs the CNIL in writing and within a maximum period of 30 calendar days from the date of termination.7.11( 3) When the certification is reinstated after suspension or when the scope of the certification is reduced, the certification body informs the CNIL in writing of its decision in accordance with the requirements of §7.6 of this standard. 7.11(4) In the case of he refusal of certification, suspension or withdrawal, the customer is informed of the options available to him to appeal this decision of the certification body, the means and the time limits available to him to make this appeal. 7.12. Records7.12(1) In addition to the requirements of §7.12 of ISO 17065, the certification body must keep records proving that the requirements of this standard have actually been met. At a minimum, this documentation must: a) Include records relating to certifications that have been issued and refused; b) Include records relating to applications for certification being processed; c) Be available over a period of 6 years, in particular s concerning the report of its evaluations (§7.4) and its monitoring activity (§7.9). In the event of a dispute between the certification body and the client or an appeal to the CNIL, the retention period for the records for the purposes of the dispute/appeal is defined according to the rules applicable to the dispute procedure concerned. ;d) Be communicated to the CNIL, at its request, in particular with regard to evaluation reports (see the requirements of §7.4(8) and 7.9(3) of this reference document). A French translation of a part of this documentation must be communicated to the CNIL at its request.7.13. Complaints and appeals7.13(1) In addition to the requirements of §7.13 of ISO 17065, the certification body shall have a documented process allowing it to receive, evaluate and take decisions relating to complaints and calls relating to its certification activity, taking into account the rules defined by the certification scheme. At a minimum, this procedure should define: a) Who can lodge a complaint or make an appeal; b) Who is responsible for collecting and verifying all the information necessary (to the extent possible) for the complaint or the appeal leads to a decision; c) Who is responsible for taking a decision to resolve the complaint or the appeal; or its appeal; e) How the audits will be carried out; f) What methods may be used to deal with the complaint or appeal, including consultation with interested parties. complainant if his complaint concerns the certification activity for which he is responsible. This confirmation is given to the complainant within a period which may not

exceed one month. If necessary, this period may be extended by an additional month. The certification body informs the complainant of this extension and the reasons for the postponement within one month of receipt of the request.7.13(3) The certification body informs the public of the procedure to be followed for file a complaint or request an appeal. This procedure must be easily accessible to the persons concerned by the processing of personal data within the scope of the certification.7.13(4) The certification body informs the complainant or the applicant of the progress of the processing and the consequences data at its request within a reasonable time, according to the conditions provided for in its documented procedure for handling complaints and appeals. When the certification body is unable to provide a solution to the complaint, it informs the complainant of its conclusion and the reasons why a resolution was not possible.7.13(5) The certification body shall ensure that the complaints and appeals management process is independent of the assessment activity certification review and decision-making to ensure that there is no conflict of interest. 7.13(6) The certification body shall undertake and maintain a register of complaints and appeals. This register must include: a) The status of the processing of each complaint or appeal (for example: received, in process, closed, etc.); b) The dates of the actions carried out (for example: acknowledgment of receipt, admissibility, informing the complainant, final response, no follow-up, etc.).8. Management system requirements8.1. General8.1(1) In addition to the requirements of §8 of ISO 17065, the certification body must establish and maintain a management system capable of guaranteeing consistent compliance with the requirements of this standard for the certification mechanisms in the scope of its approval. This implies that the implementation of these additional requirements must be documented, assessed and monitored independently to ensure compliance, transparency and the verifiable nature of compliance with the requirements of this standard. To this end, the management system must define a methodology aimed at satisfying these additional requirements and controlling them, in accordance with the regulations relating to data protection, and constantly checking them. In particular, the management system must guarantee compliance with the requirements in §4.6 (Information accessible to the public) and §7.8 (Directories of certified products) of this standard, so that it is made public, on a permanent and continuous basis, which certifications have been carried out, on what basis ( or according to which certification mechanisms or certification scheme), what is the validity period of the certifications and in what context and under what conditions (recital 100 of the GDPR).8.1(2) The operating rules of the management system and the documentation of its implementation must be presented by the certification body during the approval procedure and accessible by the CNIL at its request at any time.8.2. General documentation of the management system8.2(1) The requirements of §8.2 of ISO 17065

apply.8.3. Control of documents8.3(1) The requirements of §8.3 of ISO 17065 apply.8.4. Control of records8.4(1) The requirements of §8.4 of ISO 17065 apply.8.5. Management review8.5(1) The requirements of §8.5 of ISO 17065 apply.8.6. Internal audits8.6(1) The requirements of §8.6 of ISO 17065 apply.8.7. Corrective actions8.7(1) The requirements of §8.7 of ISO 17065 apply.8.8. Preventive actions8.8(1) The requirements of §8.8 of ISO 17065 apply.9. Other additional requirements9.1. Updating of assessment methods9.1(1) The certification body establishes procedures intended to update the assessment methods which must be applied in §7.4 of these standards. In particular, this update must be considered on the basis of changes having consequences on the certification (see requirements of §7.10 of this standard) and as a preventive action as provided for in §8.8 of ISO 17065.7 . Application rules specific to the certification mechanism Application rules specific to the certification mechanism and which are binding on the certification body within the framework of its accreditation may be defined by the certification mechanism scheme approved under the Article 42 of the GDPR. The President,

M.-L. Denis