Deliberation 2022-026 of January 27, 2022 National Commission for Computing and Liberties Legal status: In force Date of publication on Légifrance: Friday April 15, 2022 certification bodies for the certification of training providers in the protection of personal dataThe 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 relating to the protection of individuals with regard to the processing of personal data and the free movement of such data (general regulations on data protection); Having regard to law n ° 78-17 of January 6, 1978 as amended relating to the information technology, files and freedoms, in particular its articles 8 I 2° h); Considering decree n° 2019-536 of May 29, 2019 taken for the application of law n° 78-17 of January 6 January 1978 relating to data processing, files and freedoms, in particular its article 74; Having regard to deliberation n° 2020-139 of December 3, 2020 adopting the criteria of the certification reference system for training providers in the protection of personal data personnel;On the proposal of Mrs. Anne DEBET, commissioner, and after having heard the observations of Mr. Benjamin TOUZANNE, government commissioner;Adopts the requirements of a reference system relating to the approval of certification bodies for the certification of service providers training in the protection of personal data.This decision will be published in the Official Journal of the French Republic.The PresidentMarie-Laure DENISREFERENTIAL RELATING TO THE ACCREDITATION REQUIREMENTS OF CERTIFICATION BODIES FOR THE CERTIFICATION OF DATA PROTECTION TRAINING PROVIDERS TO PERSONAL CHARACTER1. WHO IS THIS GUIDELINE FOR? This reference system is intended for the certifying bodies mentioned in article 8 of the Data Protection Act which wish to obtain an authorization allowing them to certify the services of data protection training providers according to the criteria of the certification system approved by the CNIL by deliberation no. 2020-139 of December 3, 2020.2. SCOPE OF THE REFERENCE This reference lays down the requirements that the certification body must meet in order to obtain and then maintain its accreditation. It was decided, in accordance with the cooperation agreement concluded between the CNIL and the French Accreditation Committee (COFRAC), a body National Accreditation Authority, that the latter carries out the accreditation of certifying bodies. In this case, the accreditation issued by COFRAC takes the place of approval within the meaning of Article 8 of the Data Protection Act.3. ACCREDITATION PROCEDURES Obtaining accreditation according to standard EN ISO/IEC 17065 and the professional training system according to decree no. 2019-565 of June 6, 2019 is a prerequisite for submitting a file to the national accreditation body. The candidate certification body submits an accreditation application file to COFRAC or any other accreditation body that has signed a multilateral recognition agreement taken within the framework of the European

coordination of bodies Accreditation (EA). During the transitional period between the submission of its file and obtaining accreditation, the certification body is authorized to begin its certification activity provided that it has received a favorable response from the national accreditation body. following the review of its application for accreditation, called operational admissibility according to the COFRAC accreditation regulations. The certification body has a maximum 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 the certification mechanisms approved under Article 8 of the Data Protection Act.4. DURATION OF ACCREDITATION The duration of accreditation is that of the accreditation issued by the national accreditation body.5. OBLIGATIONS OF THE CERTIFICATION BODY To obtain its accreditation, the certification body must: hold an accreditation for professional training certification according to Decree No. 2019-565 of June 6, 2019, currently valid. If this accreditation is suspended, reduced or withdrawn, this automatically calls into question the accreditation relating to this standard; to be able to demonstrate to the national accreditation body its compliance with the requirements defined in part 6 of this standard; to establish a procedure in order to investigate and respond, in writing and as soon as possible, to any request for information from the CNIL concerning the supply of aggregated data relating to the certification activity (statistics) or data relating to the compliance with the requirements of this standard, in particular for the requirements relating to the handling of complaints and appeals in connection with the certification activity. The certification body is also subject to the following obligations: in the event of suspension of accreditation, it is no longer authorized to issue certificates until the suspension is lifted by the national accreditation body. During this period, the certification body must nevertheless continue to monitor valid certifications; in the event of withdrawal or termination of accreditation, cessation of certification activity, or when the certification body has been authorized to start its certification activity following the review of its application for accreditation but has not managed to obtain accreditation from the national accreditation body 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 training providers holding a certificate issued by the certification body or in the process of being certified. They choose another certifying body accredited or in the process of being accredited by a national accreditation body to transfer their certification to it.6. REQUIREMENTS TO BE MET BY CERTIFICATION BODIES Evaluation reference - Certification of training providers in the protection of personal data - Version of 27-01-20221. Scope This document includes requirements relating to

the skills, consistency of activities and impartiality of the certification bodies involved in the certification of the services of training providers in the protection of personal data according to the criteria of the certification approved by the CNIL by deliberation no. 2020-139 of December 3, 2020.2. Normative referencesEN ISO/IEC 17065: Conformity assessment – Requirements for bodies certifying products, processes and services (ISO 17065 in the remainder of this reference). By default, all the clauses of the ISO 17065 standard apply. The requirements below add specificities related to the certification of training provider services in the protection of personal data.3. Terms and definitions The terms and definitions of the EN ISO/IEC 17065:2012 standard apply. In order to facilitate the reading of this reference document, the main definitions are listed below. GDPR: General Data Protection Regulations Data Protection Act : Law No. 78-17 of 6 January 1978 as amended relating to data processing, files and freedoms CEPD: European Data Protection Committee CNIL: National Commission for Data Protection and Freedoms Certification: certificate 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 Certification process: all the activities leading to the issuance of certification and the maintenance of the validity of this attestation (eg. activities: assessment, monitoring, etc.) Audit: methodical, independent and documented process, allowing obtain objective evidence and evaluate it objectively to determine the extent to which criteria are met Audit plan (or evaluation plan): description of the activities and arrangements necessary to carry out an audit Finding (or finding): results 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 certification criteria and verifiable Non-conformity: non-satisfaction of a certification criterion audit (or evaluation report): document used to present the results of the audit Approval: certificate issued to a certification body, constituting recognition of its competence to apply the certification process and authorizing it to issue certification Certification body : conformity assessment body which carries out the tasks of the certification processE accreditation requirements: requirements to be met by the certification body when implementing the certification process in order to obtain accreditation and then maintain it (subject of this standard for the certification of protection training providers personal data)Client (or candidate): training provider who has obtained certification or who has requested it from a certification bodyProduct (or service): result of the data protection training processCall: request expressed by a client to a certification body to reconsider any unfavorable certification decision with regard to the status of the certification he has requested Complaint (or claim): any expression of dissatisfaction, other than an appeal, issued by any person or organization with a certification body,

and relating to its certification activities Transfer of certification: taking over a certificate cation existing and validated by another certification body4. General requirements4.1. Legal and contractual domain4.1.1 Legal liability4.1(1) The requirements of §4.1 of ISO 17065 apply.4.1.2 Certification contract4.1.2(1) In addition to the requirements of §4.1.2 of ISO 17065, the certification body must ensure that the contract for the provision of certification activities also contains commitments from the client on the following points: a) comply with the certification criteria for training providers 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, within the limits of 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 itions for access to documentation and records, access to necessary equipment, sites or areas, exchanges with its personnel and access to relevant information relating to its subcontractors; c) take the necessary measures to allow the participation of the CNIL and the national accreditation body in the evaluation of the client as an observer; d) inform the certification body in the event of significant changes in its legal situation or its situation of fact, of significant changes to its training offer, of any change in its training process that is likely to affect compliance with the certification criteria or any change that concerns information appearing on the official certification documentation, as provided for in §7.7 of this standard (certificate); e) authorize the certification body to communicate to the CNIL:- information relating to the issue or withdrawal of the certification in accordance with the requirements of §7.6 (Certification decision) of this reference system;- at his request, information relating to the certification procedure in accordance with the requirements of §7.12 (Records) of this reference system.4.1.2(2) The contract for the supply of certification activities must also inform the client of the following points: a) certification does not reduce the liability of its client in terms of compliance with the provisions of the GDPR and the Data Protection Act and is without prejudice 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 organization and procedures put in place by the certification body for the purpose of managing the complaints and appeals. 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; c) the rules applicable to the maintenance of the certification, its renewal, its suspension and its withdrawal, 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; d) the general consequences of arrival at the end of the accreditation period, suspension or withdrawal of accreditation. The actions available to the client to maintain the validity of the certification or to renew it are also specified. In particular, the certification body informs the client 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 of refusal, suspension or withdrawal of its accreditation for the certification of data protection training providers approved by the CNIL.4.1.3 Use of licenses, certificates and trademarks of conformity4.1.3(1) In addition to the requirements of §4.1.3 of ISO 17065, the certification body must exercise its control over the use and display of licenses, certificates and marks of conformity as well as any other device intended to identify the training process of a certified provider, ensuring that: a) the certification of data protection training providers es is clearly mentioned. In particular, the communication is transparent on the fact that it relates only to the personal data protection training offered by the service provider; b) the scope of the certification is unambiguous in order to prevent any confusion concerning the training which have been evaluated; c) the rules for the use of trademarks registered by the CNIL for certified training providers are respected. 4.1.3(2) The incorrect or ambiguous use of licenses, certificates, marks of that any other device intended to identify the training process of a certified provider must be corrected by appropriate action. At a minimum, this includes: a) the obligation for the certified training provider to take measures to put an end to incorrect or ambiguous practices; b) the obligation for the certified training provider to renew information to the public, by failing this, using means of communication 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 training provider; Note: Other appropriate actions decided by the certification body may also include the withdrawal or suspension of the 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 ensure that: a) the personnel involved in the assessment, review and certification decision-maker does not act as a designer of training content, designer of assessment methods or trainer for any of its client's data protection training courses; b) it is not affiliated with the organization of his client, nor does he belong to the same group as his client; c) he has not called on his client to train his staff in data protection for at least 2 years.4.3. Liability and financing4.3(1) The requirements of §4.3 of ISO 17065 apply.4.4. Non-discriminatory conditions4.4(1) The requirements of §4.4 of ISO 17065 apply.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 reference system); b) the information necessary for the publication by the CNIL of a directory of certified persons (see the requirements of §7.8 of this repository).4.5(2) The certification body must inform the client that, at the request of the CNIL, it may be required to send the CNIL additional information in connection with its assessment, in order to demonstrate the conformity of the certification process to the requirements of this standard (see requirements of §7.12 of this standard).4.6. Information accessible to the public4.6(1) The requirements of §4.6 of ISO 17065 apply.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 staff 6.1(1) In addition to the requirements of §6.1 of ISO 17065, the certification body shall establish, implement and maintain a competency management procedure in order to demonstrate that its staff in in charge of assessments (auditors) has the appropriate and up-to-date skills (knowledge and experience) to carry out its certification activities. In particular, the auditor must: a) have received specific training in the protection of personal data; b) have appropriate experience in the analysis and/or implementation of the applicable regulations the protection of personal data (RGPD and Data Protection Act) for the sectors of activity, specific themes or specific types of data processing operation targeted by the objectives of the training courses offered by the service provider; c) have appropriate experience in the analysis and/or implementation of technical and organizational data protection measures. Note: It is up to the certification body to define the appropriate competence criteria based on the requirements above.6.1(2) The certification body must ensure that the competence of the auditors is maintained, for example by means of a professional training programme.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 standard which apply to the assessment activity.6.2(2) In particular, when assessment activities are outsourced to another organization, the The certification body must: a) check, for each auditor, that the requirements of §6.1 of these standards are met; b) check that the personnel involved in the certification process have no other link of interest with the training provider only the certification process and has no activity related to the training activity carried out by the training provider which would be likely to call into question the impartiality of the certification body (see requirements of §4.2 of this standard).7. Process Requirements7.1. General7.1(1) The requirements of §7.1 of ISO 17065 apply. Training providers are assessed according to the criteria of the

certification reference system for training providers in the protection of personal data approved by the CNIL by deliberation no. 2020-139 of December 3, 2020. To carry out its assessment, the certification body takes into account the reading guide published by the CNIL on its website.7.2. Request7.2(1) In addition to the requirements of §7.2 of ISO 17065, the certification body must collect from the service provider: a) the list of training courses in the protection of personal data that it offers as well as , where applicable, information relating to sectors of activity or specific themes or even to particular types of data processing operation that it has identified for them; b) the list of subcontractors involved in the data protection training services; c) the information relating to the provision of the training services, including the address of the permanent places where the training is managed, designed and carried out; d) where applicable, ensures by any means of the validity of the RNQ certification obtained.7.3. Review of the application7.3(1) To examine the applications for certification 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 that it has the necessary skills in terms of data protection, in accordance with the requirements of §6 of this standard, to carry out the certification activity. data processing operation.7.3(3) The certification body implements a procedure for calculating the duration of the audit. The audit duration retained by the certification body is indicated in the certification contract. The rules applicable to the calculation of the audit durations are those defined in article 4 of the decree of June 6, 2019 relating to the terms associated with the RNQ reference system concerning training actions (for the action categories in L.6313-1-3° of the Labor Code). For the initial or renewal assessment, to the duration calculated according to the aforementioned RNQ methods (initial or renewal), there is a minimum of 1 day of assessment added for: - training providers not certified according to the RNQ reference system; - service providers certified according to the RNQ standard and who offer more than 3 training courses relating to data protection in their training catalog (or who have already carried out 3 tailor-made training courses with different training objectives). In supervision, to the duration calculated according to the aforementioned RNQ methods (supervision), is added a minimum of 0.5 day of assessment under the same conditions (i.e. for non-RNQ certified training providers and for certified providers with more than 3 courses). The certification body can reduce the durations calculated for the assessment by justifying either:- the results of an audit according to the RNQ standard;- an optimization made possible by an audit combined with the assessment of the RNQ standard;- the implementation of other applicable standards, such as registration in the National Directory of Professional Certifications (RNCP) or Specific Directory

(RS). 7.3(4) In the case of a request concerning a candidate who wishes to change certification body by requesting the transfer of its certification, the certification body must: a) verify that the candidate has a valid certificate at the time of its request; b) in addition to the information listed in §7.2 of these standards, obtain from the candidate:- a copy of the certificate issued;- the last audit report;- the complaints received. status of non-conformities pending, the findings of the last audit report, the complaints received and the corrective actions implemented; d) take its decision concerning the transfer of certification within a period of one month. all or part of the documents listed above or in case of doubt on compliance with the certification criteria, the certification body cannot transfer the certification as is and must start a new certification process starting with an initial audit, as provided for in §7.4 of these standards.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 certification body carries out its assessment on the premises of the training provider. However, in the event that the latter does not have premises dedicated to the provision of training services, the parties may agree on the location of the audit. When the assessment is carried out in addition to a pre-existing certification according to the RNQ reference system (or when it is carried out simultaneously with a view to obtaining RNQ certification), the certification body can carry out the assessment of the certification criteria approved by the CNIL remotely, provided that the conditions for taking account of RNQ certification, as defined in §7.4(6) of this standard, are complied with.7.4(2) In addition to the requirements in §7.4.5 of ISO 17065, as part of the review process for the request in §7.3 of ISO 17065, when the certification body relies on the result of an RNQ certification obtained before its assessment, the certification body must ensure that the certificate will be valid at the time of assessment.7.4(3) Lor s that the assessment is carried out in addition to the result of an RNQ certification, the certification body must ensure that the training provider complies with the certification criteria approved by the CNIL. In particular, the certification body must: a) have access to the entire audit grid according to the RNQ reference system (and not just the certificate of conformity or a similar certificate); b) document its own findings by: - referring to the relevant results of the pre-existing audit grid (the reproduction of the findings in the assessment report is not required); - making its own findings when they are necessary for the assessment of the additional criteria of the reference system certification approved by the CNIL. If deviations from the findings of the RNQ certification evaluation grid are identified by the certification body during its assessment of the additional criteria approved by the CNIL, the assessment is extended to certification criteria concerned.7.4(4) In addition to the requirements of §7.4.9 of ISO 17065, the certification body must document its findings in an evaluation report which includes:a) the list of data protection training offered

and/or carried out;b) the evaluation plan (including updates carried out during the evaluation);c) the references to the documents and records reviewed;d) the training courses sampled; e) the function of the persons interviewed; -conformities. The certification body requests the training provider to propose the implementation of measures aimed at correcting all non-conformities so that they can be taken into account by the certification body at the time of 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(5) The certification body provides the CNIL, at its request, with the report of its assessments as well as its annexes. Note: to demonstrate compliance with the requirements of this standard, the certification body is not required to keep the evidence (e.g.: documents, screenshots, etc.) that it made it possible to establish the findings documented in its assessment report.Note: In accordance with the requirements of §7.12 of this standard, the certification body keeps the report of its assessments for a period of 6 years.7.5. Review7.5(1) The requirements of §7.5 of ISO 17065 apply.7.6 Certification decision7.6(1) In addition to the requirements of §7.6 of ISO 17065, the certification body defines procedures to take certification decisions or to refuse certification. ISO 17065 or when the appropriate measures in response to a nonconformity include an evaluation in accordance with §7.11.2 of ISO 17065: renewal, suspension, lifting of suspension or withdrawal of certification. These procedures must provide that: a) the reasons which led to a favorable decision are identified and documented on the basis of objective evidence and facts; b) the reasons which led to the refusal, suspension or withdrawal of certification are identical tified and documented, particularly with regard to the seriousness, number and recurrence of the non-conformities observed. In particular, the case of major non-conformities not lifted within three months constitute reasons leading to the refusal, suspension or withdrawal of certification. This is also the case for minor nonconformities already detected and for which the organization has not proposed or implemented effective corrective actions; c) the period between the end of the assessment (last findings) and the certification decision cannot exceed 3 months, except in exceptional circumstances for which the justifications are documented; d) in addition to the review of the information relating to the RNQ certification (see requirement §7.2(1)(d) of this reference system), the certification body verifies that this certification is still valid when making the decision. In the event of suspension or withdrawal of the RNQ certification, a complete audit according to the certification criteria approved by the CNIL is carried out; e) the certification body informs the CNIL of its decisions, in writing and within a maximum period of 30 calendar days from the date of its decision, when the certification is issued (or

renewed or reinstated) or withdrawn (or suspended); The information provided to the CNIL must include: - the name of the training provider and the elements allowing its identification;- the official certification documentation, as provided for in §7.7 of these standards (the certificate issued).f) the certification body informs the training provider of the certification decisions.7.6(2) The certification body certification defines its certification procedures in such a way as to guarantee its independence and assume its responsibilities with regard to its certification decisions. In particular, the certification body must demonstrate that the person(s) it appoints to make a certification decision have not been directly or indirectly involved in the assessment process.7.7. Certification document7.7(1) In addition to the requirements of §7.7 of ISO 17065, the certification body must provide the training provider with official certification documents (certificate) which identify the name and reference (including version) of the Training Provider Certification Criteria that were used for the assessment.7.7(2) Certificates are valid for 3 years.7.8. Directories of certified services7.8(1) In addition to the requirements of §7.8 of ISO 17065, the certification body keeps up-to-date information on certified service providers, including at least: a) a reference to the version of the criteria certificates that were used for the assessment; b) the validity status of the certification: in progress (not yet issued), issued (initial certification), renewed, expired, terminated, suspended or withdrawn; c) the date on which the certification was issued (or renewed); d) the dates on which the surveillance activities were carried out; e) the date on which the certification expired or expired, or the date on which the certification was terminated , suspended or withdrawn.Note: this information does not have to be made public, contrary to the information provided for in the requirements of §7.8(2) of this reference system, but must be accessible on request from a third party who wishes to ascertain the status a certification.7 .8(2) The certification body must, at a minimum, publish the following information in a directory: a) the name of the service provider and the information enabling it to be contacted; b) the name and the reference (including the version) the certification criteria of the training providers that have been assessed; c) the date on which the certification was issued (or renewed); d) the validity status of the certification resulting from the last certification decision. it informs the CNIL of the issue of the certification (in accordance with the requirements of §7.6 of this standard), the certification body provides it with this information, which will be published.7.9 Monitoring and renewal7.9(1) The certification body must define a procedure for monitoring compliance of the training process for certified service providers with the certification criteria approved by the CNIL, in accordance with the requirements of §7.9 of ISO 17065. The monitoring audit is carried out between the 14th and 22nd month following the date of obtaining the certification. It makes it possible to verify, once the certification has been issued, that the certification criteria are still respected.

The surveillance audit is carried out remotely. However, the certification body may carry out an on-site assessment in order to establish its findings in the case of: a) reports when they meet the complaints rules defined by the certification body; b) results of an analysis from the previous audit. Note: The risk analysis carried out by the certification body as part of its surveillance activity may take into account various factors such as the increase in the volume of activity, the number and the nature of nonconformities being addressed, etc. 7.9(2) In addition to the requirements of §7.9 of ISO 17065, monitoring shall include: a) an evaluation of the changes that have been applied to the training process and to the training offer 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 where actual implementation was not applicable, for example because training in a particular sector was offered by the training provider but had not yet been carried out; c) assessment of the implementation implementation of measures provided for by the action plan resulting from the previous certification decision (see the requirements of §7.4 and §7.11 of this standard); d) an in-depth assessment of 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 evaluation can be deepened by:- the analysis of a larger quantity of evidence (training, 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 training courses carried out since the previous assessment; - the analysis of the recordings in different contexts of implementation of the training (e.g. evaluation in other physical premises of the training provider, of certain particularly personalized training processes) in order to ensure that the findings established are consistent.7.9(3) In addition to regular evaluations, monitoring measures necessary to maintain the certification must make it possible to: a) ensure that the information relating to the certification is up to date; b) the organization of an additional assessment at the initiative of the certification body, when this is proportionate to the risk. 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(4) The certification body must document the results of its monitoring activity for each certification, including its consequences when the surveillance results in a decision to suspend or withdraw the certification. Note: In accordance with the requirements

of §7.12 of this standard, the certification body keeps the records relating to its surveillance activity for a period of 6 years. 7.9(5) Where the client's request is for renewal of certification, the certification body shall follow a n certification process that complies with the same requirements of this standard as those applicable to an initial certification application. The renewal of certification assumes the performance of a renewal audit before the expiry date of the certificate. This audit follows the same procedures as those of the initial audit and has the same duration as that calculated according to the requirement of §7.3(3). It gives rise to obtaining a new certificate. The renewal decision must be made before the expiry of the certification. In the event of renewal, the new certification decision takes effect the day after the expiry date of the previous certificate. 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 changes applied to the training process and /or to the training offer which is likely to have an effect on compliance with the certification criteria approved by the CNIL; b) any modification made to the regulations relating to the protection of personal data when it is likely to have a substantial effect on the content of the training offered; c) the binding decisions or opinions of the EDPS and/or the CNIL in connection with the content of the training offer; personal data brought to its attention when they are likely to have a substantial effect on the content of the training offer; Note: the certification body may also take into account the recommendations, good practices and other documents recently adopted by the EDPS and/or the CNIL in connection with the content of the training offer.7.10(2) The certification body defines a management procedure enabling it to analyse, decide and implement changes that affect the certification process. At a minimum, this includes: a) establishing and updating a register listing the changes analyzed as having consequences on the certification process as well as the training providers concerned; b) documenting the measures decided to implement the changes having consequences on the certification, in particular:- the reasons which led to not immediately carrying out an additional evaluation or a re-evaluation of the certification criteria for the training providers concerned;- the reasons which led to no evaluation being carried out and, where applicable, the other types of actions implemented; - the rules applicable to transition periods, including when they are defined by the CNIL when updating the certification criteria for training providers , the deadlines applicable to the changes to be implemented and the conditions for maintaining or renewing the certification of format providers c) inform the training provider, 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 process training remains in compliance with the certification criteria approved by the CNIL. The planned evaluation must be proportionate to the consequences on the

certification. When a transition period is defined, the service provider is informed of the deadlines to be met in order to maintain or renew its certification, as well as the consequences in the event of non-compliance with these; d) revise the official certification documents (certificates) , suspend or withdraw certification, if the assessment concludes that the training process no longer complies with the training provider certification criteria; e) update its certification procedures so that they apply to future customers in a uniform manner.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-compliance with the certification criteria. At a minimum, this includes: a) when non-compliance with the certification criteria is proven, the certification body must determine whether the corrective actions proposed by the service provider are likely to remove the non-compliance before taking a decision to certification. This opinion is without prejudice to the conclusions of the assessment of the implementation of the measures by the service providers when it will be carried out by the certification body. For all non-conformities, the certification body assesses whether the proposed action plan makes it possible to guarantee the conformity of the service provider training process when the certification decision is made. 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:- for a minor non-conformity, the action plan must be implemented within 6 months. Verification of the implementation of corrective actions is carried out at the next audit. If the minor non-conformity is not lifted at the next audit, it is reclassified as a major non-conformity; - for a major non-conformity, verification of the implementation of the action plan must be effective under 3 months. If the corrective actions are not implemented, the certification is refused or suspended. The certification is granted or the suspension of the certification is lifted by the certification body following receipt of evidence showing the resolution of the major non-conformities and the return to compliance of the training provider. If the corrective actions are not implemented within 3 months after the refusal or suspension, the certification is withdrawn or not issued. A new application for certification then requires the performance of a new initial certification audit; c) when the certification of the service provider is conditional on the implementation of an action plan, the certification body verifies that the implementation implementation of measures to correct non-conformities is carried out according to the schedule and takes the appropriate actions when non-conformities are not resolved according to the action plan. Note: The verification of the treatment of non-conformities may give rise the performance of an additional audit, remotely or on site.7.11(2) When the certification is

terminated at the request of the training provider, the certification body informs the CNIL in writing and within a maximum period of 30 days calendar from the date of termination.7.11(3) When certification is restored after suspension, the certification body informs the CNIL of its decision in accordance with the requirements of §7.6 of the p present standard.7.11(4) In the event of a refusal of certification, suspension or withdrawal, the service provider is informed of the options available to him to appeal this decision of the certification body, the means and the deadlines for which he disposes to make this recourse.7.12. Records7.12(1) In addition to the requirements of §7.12 of ISO 17065, the certification body keeps the 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 training provider 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 procedure. litigation concerned; d) be communicated to the CNIL, at its request, in particular with regard to the assessment reports (see the requirements of §7.4(9) and 7.9(4) of these standards).7.13. Complaints and recalls7.13(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 appeals relating to its certification activity. 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 (as far as possible) for the complaint or the the appeal leads to a decision; c) who is responsible for taking a decision to find a solution to the complaint or the appeal; d) the different stages of informing the complainant about the follow-up given to his complaint; 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. appeal relates to 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 people who have made or wish to make a request for training with a certified service provider. complaint 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, review and certification 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 of service providers. data protection training approved by the CNIL. This implies that the implementation of these additional requirements must be documented, evaluated and monitored independently to ensure compliance, transparency and the verifiability of compliance with the requirements of this standard .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 accreditation procedure and accessible by the CNIL at its request.8.2. General documentation of the management system8.2(1) The requirements of §8.2 of ISO 17065 apply.8.3. Control of documents 8.3(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.