RÉFÉRENTIEL

RELATIF AUX EXIGENCES D'AGRÉMENT DES ORGANISMES DE CERTIFICATION POUR LA CERTIFICATION DES PRESTATAIRES DE FORMATION À LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

1. À qui s'adresse ce référentiel ?

Ce référentiel s'adresse aux organismes certificateurs mentionnés à l'article 8 de la loi Informatique et Libertés qui souhaitent obtenir un agrément leur permettant de certifier les services des prestataires de formation à la protection des données selon les critères du référentiel de certification approuvés par la CNIL par la délibération n° 2020-139 du 3 décembre 2020.

2. Portée du référentiel

Ce référentiel fixe les exigences que l'organisme certificateur doit respecter pour obtenir, puis conserver, son agrément.

Il a été décidé, conformément à la convention de coopération conclue entre le CNIL et le Comité français d'accréditation (COFRAC), instance nationale d'accréditation, que ce dernier procède à l'agrément des organismes certificateurs. Dans ce cas, l'accréditation délivrée par le COFRAC tient lieu d'agrément au sens de l'article 8 de la loi Informatique et Libertés.

3. Modalités d'accréditation

L'obtention de l'accréditation selon la norme EN ISO/IEC 17065 et le dispositif de la formation professionnelle selon le décret n° 2019-565 du 6 juin 2019 est un prérequis préalable au dépôt d'un dossier auprès de l'instance nationale d'accréditation.

L'organisme de certification candidat dépose un dossier de demande d'accréditation auprès du COFRAC ou de tout autre organisme d'accréditation signataire d'un accord de reconnaissance multilatéral pris dans le cadre de la coordination européenne des organismes d'accréditation (EA).

Durant la période transitoire entre le dépôt de son dossier et l'obtention de l'accréditation, l'organisme de certification est autorisé à débuter son activité de certification sous réserve qu'il ait reçu une réponse favorable de l'instance nationale d'accréditation suite à la revue de sa demande d'accréditation, appelée recevabilité opérationnelle selon le règlement d'accréditation du COFRAC.

L'organisme de certification dispose d'une période maximale de 12 mois à compter de la date de la réponse favorable du COFRAC pour obtenir l'accréditation.

La convention de coopération signée le 20 mai 2020 entre la CNIL et le COFRAC fixe les rôles, les responsabilités et les procédures opérationnelles liées à l'accréditation des organismes de certification pour les mécanismes de certification approuvés au titre de l'article 8 de la loi Informatique et Libertés.

4. Durée de l'agrément

La durée de l'agrément est celle de l'accréditation délivrée par l'instance nationale d'accréditation.

5. Obligations de l'organisme de certification

Pour obtenir son accréditation, l'organisme de certification doit :

- être titulaire d'une accréditation pour la certification de formation professionnelle selon le décret n°2019-565 du 6 juin de 2019, en cours de validité. Si cette accréditation est suspendue, réduite ou retirée, ceci remet automatiquement en cause l'accréditation relative au présent référentiel ;
- être en mesure de démontrer à l'instance nationale d'accréditation sa conformité aux exigences définies en partie 6 de ce référentiel ;
- établir une procédure afin d'investiguer et répondre, par écrit et dans les meilleurs délais, à toute demande d'information de la CNIL s'agissant de la fourniture de données agrégées relatives à l'activité de certification (statistiques) ou de données relatives à la conformité aux exigences du présent

référentiel, notamment pour les exigences relatives au traitement des plaintes et appels en lien avec l'activité de certification.

L'organisme de certification est également soumis aux obligations suivantes :

- en cas de suspension de l'accréditation, il n'est plus autorisé à délivrer de certificats jusqu'à la levée de la suspension par l'instance nationale d'accréditation. Pendant cette période, l'organisme certification doit néanmoins poursuivre la surveillance des certifications en cours de validité ;
- en cas de retrait ou résiliation de l'accréditation, de cessation de l'activité de certification, ou lorsque l'organisme de certification a été autorisé à débuter son activité de certification suite à la revue de sa demande d'accréditation mais n'est pas parvenu à obtenir une accréditation auprès de l'instance national d'accréditation dans les délais impartis, il n'est plus autorisé à délivrer de certificats. Les certificats déjà délivrés par l'organisme de certification restent valides pendant une période de 6 mois. Il doit en informer les prestataires de formation titulaires d'un certificat délivré par l'organisme de certification ou en cours de certification. Ceux-ci choisissent un autre organisme certificateur accrédité ou en cours d'accréditation par une instance nationale d'accréditation pour lui transférer leur certification.

6. Exigences à satisfaire par les organismes de certification

Référentiel d'évaluation **Certification des prestataires de formation à la protection des données à caractère personnel** **Version du 27-01-2022**
1. Domaine d'application
Le présent document comporte des exigences portant sur les compétences, la cohérence des activités et l'impartialité des organismes de certification intervenant pour la certification des services de prestataires de formation à la protection des données à caractère personnel selon les critères du référentiel de certification approuvé par la CNIL par la délibération n° 2020-139 du 3 décembre 2020.
2. Références normatives
EN ISO/IEC 17065 : « Évaluation de la conformité – Exigences pour les organismes certifiant les produits, les procédés et les services » (« ISO 17065 » dans la suite du présent référentiel). Par défaut, toutes les clauses de la norme ISO 17065 s'appliquent. Les exigences ci-dessous ajoutent des spécificités liées à la certification des services de prestataire de formation à la protection des données à caractère personnel.
3. Termes et définitions
Les termes et définitions de la norme EN ISO/IEC 17065 :2012 s'appliquent. Afin de faciliter la lecture du présent référentiel, les principales définitions sont listées ci-après.
RGPD : Règlement général sur la protection des données
Loi Informatique et Libertés : Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés
CEPD : Comité européen de la protection des données
CNIL : Commission nationale de l'informatique et des libertés

Certification : attestation délivrée par un tiers indépendant selon laquelle le respect de critères de certification a été prouvé
Critères de certification : exigences évaluables selon lesquelles l'évaluation de conformité est effectuée
Processus de certification : ensemble des activités conduisant à la délivrance de la certification et au maintien de la validité de cette attestation (p. ex. : activités d'évaluation, de surveillance, etc.)
Audit : processus méthodique, indépendant et documenté, permettant d'obtenir des preuves objectives et de les évaluer de manière objective pour déterminer dans quelle mesure des critères sont satisfaits
Plan d'audit (ou plan d'évaluation) : description des activités et des dispositions nécessaires pour réaliser un audit
Constatation (ou constat) : résultats de l'évaluation des preuves recueillies lors de l'audit, en rapport avec les critères de certification
Preuve : enregistrement, énoncés de faits ou autres informations pertinents pour les critères de certification et vérifiables
Non-conformité : non-satisfaction d'un critère de certification
Rapport d'audit (ou rapport d'évaluation) : document utilisé pour présenter les résultats de l'audit
Agrément : attestation délivrée à un organisme de certification, constituant une reconnaissance de sa compétence à appliquer le processus de certification et l'autorisant à délivrer la certification
Organisme de certification : organisme d'évaluation de la conformité qui réalise les tâches du processus de certification
Exigences d'agrément : exigences à respecter par l'organisme de certification lors de la mise en œuvre du processus de certification afin d'obtenir l'agrément et puis le conserver (objet du présent référentiel pour la certification des prestataires de formation à la protection des données à caractère personnel)
Client (ou candidat) : prestataire de formation qui a obtenu une certification ou qui en a fait la demande auprès d'un organisme de certification
Produit (ou service) : résultat du processus de formation à la protection des données
Appel : demande exprimée par un client auprès d'un organisme de certification visant à reconsidérer toute décision de certification défavorable au regard du statut de la certification qu'il a demandé
Plainte (ou réclamation) : toute expression de mécontentement, autre qu'un appel, émise par toute personne ou organisation auprès d'un organisme de certification, et relative à ses activités de certification
Transfert de la certification : reprise d'une certification existante et valide par un autre organisme de certification
4. Exigences générales
4.1 Domaine juridique et contractuel
4.1.1 Responsabilité juridique
4.1(1) Les exigences du §4.1 de l'ISO 17065 s'appliquent.

4.1.2 Contrat de certification

4.1.2(1) En complément des exigences du §4.1.2 de l'ISO 17065, l'organisme de certification doit s'assurer que le contrat de fourniture d'activités de certification contient également des engagements du client sur les points suivants :

a) se conformer aux critères de certification des prestataires de formation et mettre en œuvre les changements nécessaires à l'occasion de leur mise à jour, notamment lorsque ceux-ci sont communiqués par l'organisme de certification ;

b) fournir à l'organisme de certification les informations et l'accès aux traitements de données qui sont nécessaires à l'exécution de la procédure de certification, dans la limite du respect des mesures organisationnelles et techniques mises en œuvre pour ces traitements de données afin de s'assurer du respect du RGPD et de la loi Informatique et Libertés ;

Cela inclut des dispositions pour l'accès à la documentation et aux enregistrements, l'accès aux équipements, sites ou zones nécessaires, l'échange avec son personnel et l'accès aux informations pertinentes relatives à ses sous-traitants ;

c) prendre les dispositions nécessaires pour permettre la participation de la CNIL et de l'instance nationale d'accréditation à l'évaluation du client en tant qu'observateur ;

d) informer l'organisme de certification dans le cas de changements significatifs de sa situation légale ou de sa situation de fait, de changements significatifs de son offre de formation, de tout changement de son processus de formation qui est susceptible d'affecter la conformité aux critères de certification ou tout changement qui concerne des informations figurant sur la documentation de certification officielle, telle que prévue au §7.7 du présent référentiel (certificat) ;

e) autoriser l'organisme de certification à communiquer à la CNIL :

- les informations relatives à la délivrance ou au retrait de la certification conformément aux exigences du §7.6 (Décision de certification) du présent référentiel ;
- sur sa demande, les informations relatives à la procédure de certification conformément aux exigences du §7.12 (Enregistrements) du présent référentiel.

4.1.2(2) Le contrat de fourniture d'activités de certification doit également informer le client des points suivants :

a) la certification ne réduit pas la responsabilité de son client en matière de conformité aux dispositions du RGPD et de la loi Informatique et Libertés et est sans préjudice de l'exercice des missions et des pouvoirs de la CNIL prévus notamment aux articles 20 à 23 de la loi Informatique et Libertés ;

b) de l'organisation et des procédures mises en place par l'organisme de certification pour le besoin de la gestion des plaintes et des appels. L'organisme de certification doit également s'assurer que le contrat engage le client à se conformer aux règles prévues par ces procédures s'agissant de l'instruction des réclamations prévue au §4.2.2.2 de la norme ISO 17065 ;

c) des règles applicables au maintien de la certification, à son renouvellement, à sa suspension et à son retrait, y compris les règles relatives aux intervalles de surveillance et de réévaluation de la certification conformément aux exigences du §7.9 du présent référentiel ;

d) des conséquences générales d'une arrivée au terme de la période d'accréditation, d'une suspension ou d'un retrait de l'accréditation. Les actions dont dispose le client pour maintenir la validité de la certification ou la renouveler sont également précisées.

En particulier, l'organisme de certification informe le client des conditions générales applicables au transfert d'une certification et de la procédure applicable dans le cas où il fait l'objet d'une décision de refus, de suspension ou de retrait de son accréditation pour la certification des prestataires de formation à la protection des données approuvée par la CNIL.

4.1.3 Utilisation de licences, de certificats et de marques de conformité

4.1.3(1) En complément des exigences du §4.1.3 de l'ISO 17065, l'organisme de certification doit exercer son contrôle sur l'utilisation et l'affichage des licences, des certificats et des marques de conformité ainsi que tout

autre dispositif destiné à identifier le processus de formation d'un prestataire bénéficiant d'une certification, en s'assurant que :

a) la certification des prestataires de formation à la protection des données est clairement mentionnée. En particulier, la communication est transparente sur le fait que celle-ci se rapporte uniquement aux formations à la protection des données à caractère personnel proposées par le prestataire ;

b) le périmètre de la certification est sans ambiguïté afin de prévenir tout confusion concernant les formations qui ont été évaluées ;

c) les règles d'usage des marques déposées par la CNIL à destination des prestataires de formation certifiés sont respectées.

4.1.3(2) L'usage incorrect ou ambigu de licences, certificats, marques de conformité, ainsi que tout autre dispositif destiné à identifier le processus de formation d'un prestataire bénéficiant d'une certification doit être corrigé par une action appropriée. *A minima*, cela inclut :

a) l'obligation pour le prestataire de formation certifié de prendre des mesures pour mettre fin aux pratiques incorrectes ou ambigües ;

b) l'obligation pour le prestataire de formation certifié de renouveler l'information du public, par défaut, en utilisant des moyens de communication similaires à ceux utilisés précédemment ;

c) l'information de la CNIL, dans les meilleurs délais, des pratiques non-conformes constatées et des actions menées par l'organisme de certification et le prestataire de formation.

Note : D'autres actions appropriées décidées par l'organisme de certification peuvent également comprendre le retrait ou la suspension de la certification, une communication relative à la faute commise ou encore, si nécessaire, l'exercice d'une action devant les juridictions compétentes.

4.2 Gestion de l'impartialité

4.2(1) En complément des exigences du §4.2 de l'ISO 17065, l'organisme de certification doit s'assurer que :

a) le personnel impliqué dans les procédures d'évaluation, de revue et de prise de décision de certification n'intervient pas en tant que concepteur du contenu des formations, concepteur des modalités d'évaluation ou formateur pour l'une des formations à la protection des données de son client ;

b) il n'est pas affilié à l'organisation de son client, ni n'appartient au même groupe que son client ;

c) il n'a pas fait appel à son client pour former son personnel à la protection des données depuis au moins 2 ans.

4.3 Responsabilité et financement

4.3(1) Les exigences du §4.3 de l'ISO 17065 s'appliquent.

4.4 Conditions non discriminatoires

4.4(1) Les exigences du §4.4 de l'ISO 17065 s'appliquent.

4.5 Confidentialité

4.5(1) En complément des exigences du §4.5 de l'ISO 17065, l'organisme de certification doit informer le client des informations qui seront fournies à la CNIL pour le besoin de la mise en œuvre du processus de certification. Cela inclut les informations suivantes :

a) les décisions de certification (voir les exigences du §7.6 du présent référentiel) ;

b) les informations nécessaires à la publication par la CNIL d'un annuaire des certifiés (voir les exigences au §7.8 du présent référentiel).

4.5(2) L'organisme de certification doit informer le client que, sur demande de la CNIL, il peut être amené à transmettre à la CNIL des informations supplémentaires en lien avec son évaluation, dans le but de démontrer la conformité du processus de certification aux exigences du présent référentiel (voir exigences du §7.12 du présent référentiel).

4.6 Informations accessibles au public

4.6(1) Les exigences du §4.6 de l'ISO 17065 s'appliquent.

5. Exigences structurelles

5.1 Organisation et direction

5.1(1) Les exigences du §5.1 de l'ISO 17065 s'appliquent.

5.2 Dispositif de préservation de l'impartialité

5.2(1) Les exigences du §5.2 de l'ISO 17065 s'appliquent.

6. Exigences relatives aux ressources

6.1 Personnel de l'organisme de certification

6.1(1) En complément des exigences du §6.1 de l'ISO 17065, l'organisme de certification doit instaurer, mettre en œuvre et maintenir une procédure de gestion des compétences afin de démontrer que son personnel en charge des évaluations (auditeurs) dispose des compétences appropriées et actualisées (connaissance et expérience) pour mener à bien ses activités de certification. En particulier, l'auditeur doit :

a) avoir bénéficié d'une formation spécifique à la protection des données à caractère personnel ;

b) disposer d'une expérience appropriée en matière d'analyse et/ou de mise en œuvre de la réglementation applicable à la protection des données à caractère personnel (RGPD et loi Informatique et Libertés) pour les secteurs d'activité, les thématiques particulières ou les types particuliers d'opération de traitement de données visés par les objectifs des formations proposées par le prestataire ;

c) disposer d'une expérience appropriée en matière d'analyse et/ou de mise en œuvre de mesures techniques et organisationnelles de protection des données.

Note : Il revient à l'organisme de certification de définir les critères de compétences appropriés en se basant sur les exigences ci-dessus.

6.1(2) L'organisme de certification doit s'assurer du maintien des compétences des auditeurs, par exemple au moyen d'un programme de formation professionnelle.

6.2 Ressources pour l'évaluation

6.2(1) En complément des exigences du §6.2 de l'ISO 17065, l'organisme de certification doit s'assurer que les organismes auprès desquels sont externalisées des activités d'évaluation, et le personnel auquel ceux-ci font appel pour réaliser ces activités, répondent aux exigences du présent référentiel qui s'appliquent à l'activité d'évaluation.

6.2(2) En particulier, quand des activités d'évaluation sont externalisées auprès d'un autre organisme, l'organisme de certification doit :

a) vérifier, pour chaque auditeur, que les exigences du §6.1 du présent référentiel sont respectées ;

b) contrôler que le personnel impliqué dans le processus de certification n'a pas d'autre lien d'intérêt avec le prestataire de formation que le processus de certification et n'a pas d'activité en lien avec l'activité de formation réalisée par le prestataire de formation qui serait susceptible de remettre en cause l'impartialité de l'organisme de certification (voir exigences du §4.2 du présent référentiel).

7. Exigences relatives aux processus

7.1 Généralités

7.1(1) Les exigences du §7.1 de l'ISO 17065 s'appliquent.

Les prestataires de formation sont évalués selon les critères du référentiel de certification des prestataires de formation à la protection des données à caractère personnel approuvés par la CNIL par la délibération n° 2020-139 du 3 décembre 2020.

Pour réaliser son évaluation, l'organisme de certification prend en compte le guide de lecture publié par la CNIL sur son site web.

7.2 Demande

7.2(1) En complément des exigences du §7.2 de l'ISO 17065, l'organisme de certification doit collecter auprès du prestataire :

a) la liste des formations à la protection des données à caractère personnel qu'il propose ainsi que, le cas échéant, les informations relatives à des secteurs d'activité ou des thématiques spécifiques ou encore à des types particuliers d'opération de traitement de données qu'il a identifié pour celles-ci ;

b) la liste des sous-traitants impliqués dans les prestations de formation à la protection des données ;

c) les informations relatives à la réalisation des prestations de formation, incluant l'adresse des lieux permanents de gestion, conception et réalisation des formations ;

d) le cas échéant, s'assure par tout moyen de la validité de la certification RNQ obtenue.

7.3 Revue de la demande

7.3(1) Pour instruire les demandes de certification selon les exigences du §7.3 de l'ISO 17065, l'organisme de certification doit prendre en considération les informations obtenues au §7.2 du présent référentiel.

7.3(2) En complément des exigences du §7.3.1 de l'ISO 17065, l'organisme de certification doit effectuer une revue des informations obtenues afin de garantir qu'il possède les compétences nécessaires en matière de protection des données, conformément aux exigences du §6 du présent référentiel, pour réaliser l'activité de certification.

Cela inclut les compétences nécessaires à l'évaluation des formations proposées par le prestataire de formation lorsqu'elles portent sur des secteurs d'activité ou des thématiques spécifiques ou encore sur des types particuliers d'opération de traitement de données**.**

7.3(3) L'organisme de certification met en place une procédure de calcul de la durée d'audit. La durée d'audit retenue par l'organisme de certification est indiquée dans le contrat de certification.

Les règles applicables au calcul des durées de l'audit sont celle définies à l'article 4 de l'arrêté du 6 juin 2019 relatif aux modalités d'audit associées au référentiel RNQ concernant les actions de formation (pour les catégories d'action au L.6313-1-3° du code du travail).

Pour l'évaluation initiale ou en renouvellement, à la durée calculée selon les modalités RNQ précitées (initial ou renouvellement), s'ajoute *a minima* 1 jour d'évaluation pour :

- les prestataires de formation non certifiés selon le référentiel RNQ ;
- les prestataires certifiés selon le référentiel RNQ et qui proposent plus de 3 formations relatives à la protection des données dans leur catalogue de formation (ou qui ont déjà réalisé 3 formations sur-mesure avec des objectifs de formation différents).

En surveillance, à la durée calculée selon les modalités RNQ précitées (surveillance), s'ajoute *a minima* 0,5 jour d'évaluation selon les mêmes conditions (à savoir pour les prestataire de formation non-certifiés RNQ et pour les prestataires certifiés avec plus de 3 formations).

L'organisme de certification peut réduire les durées calculées pour l'évaluation en justifiant soit :

- de résultats d'un audit selon le référentiel RNQ ;

- d'une optimisation rendue possible par un audit combiné avec l'évaluation du référentiel RNQ ;
- de la mise en œuvre d'autres référentiels applicables, telle que l'inscription au Répertoire National des Certifications Professionnelles (RNCP) ou Répertoire Spécifique (RS).

7.3(4) Dans le cas d'une demande concernant un candidat qui souhaite changer d'organisme de certification en demandant le transfert de sa certification, l'organisme de certification doit :

a) vérifier que le candidat dispose d'un certificat valide au moment de sa demande ;

b) outre les informations listées au §7.2 du présent référentiel, obtenir auprès du candidat :

- une copie du certificat émis ;
- le dernier rapport d'audit ;
- les plaintes reçues.

c) outre la revue prévue au §7.3(2) du présent référentiel, examiner, par une revue documentaire, l'état des non-conformités en suspens, les constats du dernier rapport d'audit, les plaintes reçues et les actions correctives mises en œuvre ;

d) prendre sa décision concernant le transfert de la certification sous un délai d'un mois.

Note : À défaut de la réception de tout ou partie des documents listés ci-dessus ou en cas de doute sur la conformité par rapport aux critères de certification, l'organisme de certification ne pourra pas transférer la certification en l'état et devra débuter un nouveau processus de certification en commençant par un audit initial, tel que prévu au §7.4 du présent référentiel.

7.4 Évaluation

7.4(1) En complément des exigences du §7.4 de l'ISO 17065, l'organisme de certification doit disposer d'un plan d'évaluation (plan d'audit).

L'organisme de certification réalise son évaluation dans les locaux du prestataire de formation. Toutefois, dans le cas où celui-ci ne dispose pas de locaux dédiés à la réalisation des prestations de formation, les parties peuvent convenir du lieu de réalisation de l'audit.

Lorsque l'évaluation est réalisée en complément d'une certification préexistante selon le référentiel RNQ (ou lorsque qu'elle est réalisée simultanément en vue d'obtenir la certification RNQ), l'organisme de certification peut réaliser l'évaluation des critères de certification approuvés par la CNIL à distance, sous réserve que les conditions de prise en compte de la certification RNQ, telles que définies au §7.4(6) du présent référentiel, soient respectées.

7.4(2) En complément des exigences au §7.4.5 de l'ISO 17065, dans le cadre du processus de revue de la demande au §7.3 de l'ISO 17065, lorsque l'organisme de certification s'appuie sur le résultat d'une certification RNQ obtenue avant son évaluation, l'organisme de certification doit s'assurer que le certificat sera valide au moment de l'évaluation.

7.4(3) Lorsque l'évaluation est réalisée en complément du résultat d'une certification RNQ, l'organisme de certification doit s'assurer de la conformité du prestataire de formation aux critères de certification approuvé par la CNIL. En particulier, l'organisme de certification doit :

a) avoir accès à la totalité de la grille d'audit selon le référentiel RNQ (et pas uniquement au certificat de conformité ou à une attestation similaire) ;

b) documenter ses propres constats en :

- faisant référence aux résultats pertinents de la grille d'audit préexistante (la reproduction des constats dans le rapport d'évaluation n'est pas requise) ;
- réalisant ses propres constatations lorsqu'elles sont nécessaires pour l'évaluation des critères complémentaires du référentiel de certification approuvé par la CNIL.

Si des écarts par rapport aux constats de la grille d'évaluation de la certification RNQ sont identifiés par l'organisme de certification lors de son évaluation des critères complémentaires approuvés par la CNIL, l'évaluation est étendue aux critères de certification concernés.

7.4(4) En complément des exigences du §7.4.9 de l'ISO 17065, l'organisme de certification doit documenter ses constats dans un rapport d'évaluation qui comprend :

a) la liste des formations à la protection des données proposées et/ou réalisées ;

b) le plan d'évaluation (incluant les mises à jour réalisées pendant l'évaluation) ;

c) les références aux documents et enregistrements examinés ;

d) les formations échantillonnées ;

e) la fonction des personnes ayant fait l'objet d'un entretien ;

f) une description des non-conformités qui identifie les critères de certification qui ne sont pas atteints et qui évalue la sévérité et la portée des non-conformités.

L'organisme de certification sollicite le prestataire de formation afin qu'il propose la mise en œuvre de mesures visant à corriger toutes les non-conformités pour qu'elles puissent être prises en compte par l'organisme de certification au moment de sa décision de certification (voir exigence au §7.6 de l'ISO 17065). Le plan d'action résultant de la décision de certification est également annexé au rapport d'évaluation. Ce plan d'action est examiné par l'organisme de certification avant la revue et la décision de certification.

7.4(5) L'organisme de certification fournit à la CNIL, à sa demande, le rapport de ses évaluations ainsi que ses annexes.

Note : pour démontrer la conformité aux exigences du présent référentiel, il n'est pas requis de l'organisme de certification qu'il conserve les éléments de preuves (p. ex. : documents, captures d'écran, etc.) qui lui ont permis d'établir les constatations documentées dans son rapport d'évaluation.

Note : Conformément aux exigences du §7.12 du présent référentiel, l'organisme de certification conserve le rapport de ses évaluations pendant une période de 6 ans.

7.5 Revue

7.5(1) Les exigences du §7.5 de l'ISO 17065 s'appliquent.

7.6 Décision de certification

7.6(1) En complément des exigences du §7.6 de l'ISO 17065, l'organisme de certification définit des procédures pour prendre des décisions de certification ou refuser la certification.

L'organisme de certification définit également des procédures pour prendre d'autres décisions relatives à la certification intervenant suite à une évaluation menée dans le cadre du processus de surveillance prévu au §7.9.2 de l'ISO 17065 ou lorsque les mesures appropriées en réponse à une non-conformité comportent une évaluation conformément au §7.11.2 de l'ISO 17065 : le renouvellement, la suspension, la levée d'une suspension ou le retrait de la certification.

Ces procédures doivent prévoir que :

a) les motifs qui ont conduit à une décision favorable sont identifiés et documentés à partir de preuves et faits objectifs ;

b) les motifs qui ont conduit au refus, à la suspension ou au retrait de la certification sont identifiés et documentés, notamment au regard de la gravité, du nombre et de la récurrence des non-conformités constatées. En particulier, le cas de non conformités majeures non levés sous trois mois constituent des raisons conduisant au refus, à la suspension ou au retrait de la certification. C'est également le cas pour les non conformités mineures déjà détectées et pour lesquelles l'organisme n'a pas proposé ou mis en œuvre d'actions correctives efficaces ;

c) la période entre la fin de l'évaluation (dernières constatations) et la décision de certification ne peut excéder 3 mois, sauf circonstances exceptionnelles pour lesquelles les justifications sont documentées ;

d) en complément de la revue des informations relatives à la certification RNQ (voir exigence §7.2(1)(d) du présent référentiel), l'organisme de certification vérifie que cette certification est toujours valide lors de la prise de décision. En cas de suspension ou de retrait de la certification RNQ, un audit complet selon les critères de certification approuvé par la CNIL est réalisé ;

e) l'organisme de certification informe la CNIL de ses décisions, par écrit et dans un délai maximal de 30 jours calendaires à compter de la date de sa décision, lorsque la certification est délivrée (ou renouvelée ou rétablie) ou retirée (ou suspendue) ;

L'information fournie à la CNIL doit inclure :

- le nom du prestataire de formation et les éléments permettant son identification ;
- la documentation de certification officielle, telle que prévue au §7.7 du présent référentiel (le certificat émis).

f) l'organisme de certification informe le prestataire de formation des décisions de certification.

7.6(2) L'organisme de certification définit ses procédures de certification de manière à garantir son indépendance et assumer ses responsabilités vis à vis de ses décisions de certification. En particulier, l'organisme de certification doit démontrer que la ou les personnes qu'il missionne pour prendre une décision de certification n'ont pas été impliquées directement ou indirectement dans le processus d'évaluation.

7.7 Document de certification

7.7(1) En complément des exigences du §7.7 de l'ISO 17065, l'organisme de certification doit fournir au prestataire de formation des documents de certification officiels (certificat) qui permettent d'identifier le nom et la référence (y compris la version) des critères de certification des prestataires de formation qui ont été utilisés pour l'évaluation.

7.7(2) Les certificats ont une durée de validité de 3 ans.

7.8 Annuaires des services certifiés

7.8(1) En complément des exigences du §7.8 de l'ISO 17065, l'organisme de certification tient à jour des informations sur les prestataires certifiés, comportant au moins :

a) une référence à la version des critères de certification qui ont été utilisés pour l'évaluation ;

b) l'état de validité de la certification : en cours (pas encore délivrée), délivrée (certification initiale), renouvelée, expirée, résiliée, suspendue ou retirée ;

c) la date à laquelle la certification a été délivrée (ou renouvelée) ;

d) les dates auxquelles les activités de surveillance ont été réalisées ;

e) la date d'échéance ou d'expiration de la certification, ou la date à laquelle la certification a été résiliée, suspendue ou retirée.

Note : ces informations n'ont pas à être rendues publiques, contrairement aux informations prévues aux exigences du §7.8(2) du présent référentiel mais doivent être accessibles sur demande d'un tiers qui souhaite s'assurer du statut d'une certification.

7.8(2) L'organisme de certification doit, *a minima*, publier dans un annuaire les informations suivantes :

a) le nom du prestataire et les informations permettant de le contacter ;

b) le nom et la référence (y compris la version) des critères de certification des prestataires de formation qui ont été évalués ;

c) la date à laquelle la certification a été délivrée (ou renouvelée) ;

d) l'état de validité de la certification qui résulte de la dernière décision de certification.

Lorsqu'il informe la CNIL de la délivrance de la certification (conformément aux exigences du §7.6 du présent référentiel), l'organisme de certification lui fournit ces informations, qui seront publiées.

7.9 Surveillance et renouvellement

7.9(1) L'organisme de certification doit définir une procédure de surveillance de la conformité du processus de formation des prestataires certifiés aux critères de certification approuvés par la CNIL, conformément aux exigences du §7.9 de l'ISO 17065.

L'audit de surveillance est réalisé entre le 14e et le 22e mois suivant la date d'obtention de la certification. Il permet de vérifier, une fois la certification délivrée, que les critères de certification sont toujours respectés.

L'audit de surveillance est réalisé à distance. Toutefois, l'organisme de certification peut réaliser une évaluation sur site afin d'établir ses constats dans les cas de :

a) signalements lorsqu'ils répondent aux règles de réclamations définies par l'organisme de certification ;

b) résultats d'une analyse de risque issue de l'audit précédent.

Note : L'analyse de risque réalisée par l'organisme de certification dans le cadre de son activité de surveillance peut prendre en compte différents facteurs comme l'augmentation du volume d'activité, le nombre et la nature de non-conformités en cours de traitement, etc.

7.9(2) En complément des exigences du §7.9 de l'ISO 17065, la surveillance doit inclure :

a) une évaluation des changements qui ont été appliqués au processus de formation et à l'offre de formation depuis la précédente évaluation et leur impact potentiel sur la conformité aux critères de certification ;

b) une évaluation des critères de certification dont les modalités de mise en œuvre ont été évaluées lors du précédent audit mais pour lesquelles la mise œuvre effective n'était pas applicable, par exemple du fait qu'une formation portant sur un secteur particulier était proposée par le prestataire de formation mais n'avait pas encore été réalisée ;

c) l'évaluation de la mise en œuvre de mesures prévues par le plan d'action résultant de la précédente décision de certification (voir les exigences des §7.4 et §7.11 du présent référentiel) ;

d) une évaluation approfondie de critères de certification sélectionnés à partir des risques de non-conformités observés lors des précédentes évaluations (mais qui n'ont pas fait l'objet d'un constat de non-conformité). Par exemple, une évaluation peut être approfondie par :

- l'analyse en quantité plus importantes d'éléments de preuve (formation, contrats, interviews, etc.) afin de consolider les constats déjà établis ;
- l'analyse des enregistrements récents afin de s'assurer que les constats établis restent valides dans le temps, par exemple une évaluation de la conformité aux critères de certification d'une ou plusieurs formations réalisées depuis la précédente évaluation ;
- l'analyse des enregistrements dans différents contextes de mise en œuvre des formations (ex : évaluation dans d'autres locaux physiques du prestataire de formation, de certains processus de formation particulièrement personnalisés) afin de s'assurer que les constats établis sont cohérents.

7.9(3) En complément des évaluations régulières, les mesures de surveillance nécessaires au maintien de la certification doivent permettre :

a) de s'assurer que les informations relatives à la certification sont actualisées ;

b) l'organisation d'une évaluation complémentaire à l'initiative de l'organisme de certification, lorsque cela est proportionné au risque. Par exemple, une évaluation complémentaire peut intervenir lorsqu'une non-conformité est suspectée du fait d'une ou plusieurs réclamations reçues par l'organisme de certification ou d'informations relatives à des pratiques non-conformes qui ont été rendues publiques ou encore lorsque cela est nécessaire pour fournir à la CNIL les informations demandées relatives à la conformité aux exigences d'agrément du présent référentiel.

7.9(4) L'organisme de certification doit documenter les résultats de son activité de surveillance pour chaque certification, y compris ses conséquences lorsque la surveillance aboutit à une décision de de suspension ou de retrait de la certification.

Note : Conformément aux exigences du §7.12 du présent référentiel, l'organisme de certification conserve les enregistrements relatifs à son activité de surveillance pendant une période de 6 ans.

7.9(5) Lorsque la demande du client porte sur le renouvellement de la certification, l'organisme de certification doit suivre un processus de certification qui respecte les mêmes exigences du présent référentiel que celles applicables à une demande de certification initiale.

Le renouvellement de la certification suppose la réalisation d'un audit de renouvellement avant la date d'échéance du certificat. Cet audit suit les mêmes modalités que celles de l'audit initial et a la même durée que celle calculée selon l'exigence du §7.3(3). Il donne lieu à l'obtention d'un nouveau certificat. La décision de renouvellement doit intervenir avant l'expiration de la certification. En cas de renouvellement, la nouvelle décision de certification prend effet le lendemain de la date d'échéance du précédent certificat.

7.10 Changements ayant des conséquences sur la certification

7.10(1) En complément des exigences du §7.10 de l'ISO 17065, les changements à prendre en compte par l'organisme de certification doivent inclure :

a) tout changement appliqué au processus de formation et/ou à l'offre de formation qui est susceptible d'avoir un effet sur la conformité aux critères de certification approuvés par la CNIL ;

b) toute modification apportée à la réglementation relative à la protection des données à caractère personnel lorsqu'elle est susceptible d'avoir un effet substantiel sur le contenu des formations proposées ;

c) les décisions ou avis contraignants du CEPD et/ou de la CNIL en lien avec le contenu de l'offre de formation ;

d) les décisions de justice en matière de protection des données à caractère personnel portées à sa connaissance lorsqu'elles sont susceptibles d'avoir un effet substantiel sur le contenu de l'offre de formation.

Note : l'organisme de certification peut également prendre en compte les recommandations, bonnes pratiques et autres documents récemment adoptés par le CEPD et/ou la CNIL en lien avec le contenu de l'offre de formation.

7.10(2) L'organisme de certification définit une procédure de gestion lui permettant d'analyser, décider et mettre en œuvre les changements ayant des conséquences sur le processus de certification. *A minima*, cela inclut :

a) établir et mettre à jour un registre répertoriant les changements analysés comme ayant des conséquences sur le processus de certification ainsi que les prestataires de formation concernés ;

b) documenter les mesures décidées pour mettre en œuvre les changements ayant des conséquences sur la certification, en particulier :

- les motifs qui ont conduit à ne pas réaliser immédiatement une évaluation complémentaire ou une réévaluation des critères de certification pour les prestataires de formation concernés ;
- les motifs qui ont conduit à ne réaliser aucune évaluation et, le cas échéant, les autres types d'actions mises en œuvre ;
- les règles applicables aux périodes de transition, y compris lorsqu'elles sont définies par la CNIL à l'occasion d'une mise à jour des critères de certification des prestataires de formation, les délais applicables aux changements à mettre en œuvre et les conditions pour maintenir ou renouveler la certification des prestataires de formation concernés.

c) informer le prestataire de formation, en temps opportun, quand les changements ayant des conséquences sur sa certification vont nécessiter une évaluation et ce qu'il sera nécessaire d'évaluer (et comment) afin de s'assurer que le processus de formation demeure en conformité avec les critères de certification approuvé par la CNIL. L'évaluation planifiée doit être proportionnée aux conséquences sur la certification. Lorsqu'une période de transition est définie, le prestataire est informé des échéances à respecter pour maintenir ou renouveler sa certification, ainsi que des conséquences en cas de non-respect de celles-ci ;

d) réviser les documents officiels de certification (certificats), suspendre ou retirer la certification, si l'évaluation conclut que le processus de formation n'est plus conforme aux critères de certification des prestataires de formation ;

e) mettre à jour ses procédures de certification de manière à ce qu'elles s'appliquent aux futurs clients de manière uniforme.

7.11 Résiliation, suspension ou retrait de la certification

7.11(1) En complément des exigences du §7.11 de l'ISO 17065, l'organisme de certification doit définir une procédure de gestion des non-conformités aux critères de certification. *A minima*, cela inclut :

a) lorsqu'une non-conformité aux critères de certification est avérée, l'organisme de certification doit déterminer si les actions correctives proposées par le prestataire sont susceptibles de lever la non-conformité avant la prise de décision de certification. Cet avis est sans préjudice des conclusions de l'évaluation de la mise en œuvre des mesures par les prestataires lorsqu'elle sera réalisée par l'organisme de certification.

Pour l'ensemble des non-conformités, l'organisme de certification évalue si le plan d'action proposé permet de garantir la conformité du processus de formation des prestataires au moment de la prise de décision de certification. Si le plan d'action n'est pas suffisant pour le garantir, l'organisme de certification doit attendre des preuves de mise en œuvre des actions correctives pour délivrer la certification ;

b) l'organisme de certification fixe un délai de mise en œuvre des actions correctives en fonction du niveau de gravité des non-conformités :

- pour une non-conformité mineure, le plan d'action doit être mis en œuvre dans un délai de 6 mois. La vérification de la mise en œuvre des actions correctives est réalisée à l'audit suivant. Si la non-conformité mineure n'est pas levée à l'audit suivant, elle est requalifiée en non-conformité majeure ;
- pour une non-conformité majeure, la vérification de la mise en œuvre du plan d'action doit être effective sous 3 mois. À défaut de mise en œuvre des actions correctives, la certification est refusée ou suspendue. La certification est octroyée ou la suspension de la certification est levée par l'organisme de certification suite à la réception de preuves permettant de constater la résolution des non-conformités majeures et le retour en conformité du prestataire de formation. À défaut de mise en œuvre des actions correctives dans un délai de 3 mois après le refus ou la suspension, la certification est retirée ou elle n'est pas délivrée. Une nouvelle demande de certification nécessite alors la réalisation d'un nouvel audit initial de certification ;

c) lorsque la certification du prestataire est conditionnée à la mise en œuvre d'un plan d'action, l'organisme de certification vérifie que la mise en œuvre des mesures visant à corriger les non-conformités est effectuée selon le calendrier prévu et prend les actions appropriées lorsque les non-conformités ne sont pas résolues selon le plan d'action.

Note : La vérification du traitement des non-conformités peut donner lieu à la réalisation d'un audit complémentaire, à distance ou sur site.

7.11(2) Lorsque la certification est résiliée à la demande du prestataire de formation, l'organisme de certification informe la CNIL par écrit et dans un délai maximal de 30 jours calendaires à compter de la date de la résiliation.

7.11(3) Lorsque la certification est rétablie après suspension, l'organisme de certification informe la CNIL de sa décision conformément aux exigences du §7.6 du présent référentiel.

7.11(4) Dans le cas d'un refus de certification, de suspension ou retrait, le prestataire est informé des options dont il dispose pour faire appel de cette décision de l'organisme de certification, des moyens et des délais dont il dispose pour effectuer ce recours.

7.12 Enregistrements

7.12(1) En complément des exigences du §7.12 de l'ISO 17065, l'organisme de certification conserve les enregistrements prouvant que les exigences du présent référentiel ont été effectivement respectées. *A minima*, cette documentation doit :

a) inclure les enregistrements relatifs aux certifications qui ont été délivrées et refusées ;

b) inclure les enregistrements relatifs aux demandes de certification en cours de traitement ;

c) être disponible sur une période de 6 ans, notamment s'agissant du rapport de ses évaluations (§7.4) et son activité de surveillance (§7.9). Dans le cas d'un contentieux entre l'organisme de certification et le prestataire de formation ou d'un recours auprès de la CNIL, la période de conservation des enregistrements pour le besoin du contentieux/recours est définie selon les règles applicables à la procédure contentieuse concernée ;

d) être communicable à la CNIL, à sa demande, notamment s'agissant des rapports d'évaluations (voir les exigences du §7.4(9) et 7.9(4) du présent référentiel).

7.13 Plaintes et appels

7.13(1) En complément des exigences du §7.13 de l'ISO 17065, l'organisme de certification doit disposer d'un processus documenté lui permettant de recevoir, d'évaluer et de prendre des décisions relatives aux plaintes et appels relatifs à son activité de certification. *A minima*, cette procédure doit définir :

a) qui peut déposer une plainte ou faire un appel ;

b) qui est responsable de la collecte et de la vérification de toutes les informations nécessaires (dans la mesure du possible) pour que la plainte ou l'appel aboutisse à une décision ;

c) qui est responsable de prendre une décision permettant d'apporter une solution à la plainte ou l'appel ;

d) les différentes étapes d'information du plaignant quant aux suites données à sa plainte ;

e) comment les vérifications seront réalisées ;

f) quelles sont les méthodes qui peuvent être engagées pour traiter la plainte ou l'appel, y compris la consultation de parties intéressées.

7.13(2) L'organisme de certification confirme au plaignant si sa plainte ou son appel concerne l'activité de certification dont il est responsable. Cette confirmation est donnée au plaignant dans un délai qui ne peut excéder un mois. Au besoin, ce délai peut être prolongé d'un mois supplémentaire. L'organisme de certification informe le plaignant de cette prolongation et des motifs du report dans un délai d'un mois à compter de la réception de la demande.

7.13(3) L'organisme de certification informe le public de la procédure à suivre pour renseigner une plainte ou faire une demande d'appel. Cette procédure doit être facile d'accès aux personnes ayant fait ou souhaitant faire une demande de formation chez un prestataire certifié.

7.13(4) L'organisme de certification informe le plaignant de l'avancée du traitement et des conclusions du processus du traitement de sa plainte dans un délai raisonnable, selon les conditions prévues par sa procédure documentée de traitement des plaintes et appels.

Lorsque l'organisme de certification n'est pas en mesure d'apporter une solution à la plainte, il informe le plaignant de sa conclusion et les raisons pour lesquelles une résolution n'a pas été possible.

7.13(5) L'organisme de certification doit s'assurer que le processus de gestion des plaintes et appels est indépendant de l'activité d'évaluation, de revue et de prise de décision de certification afin de garantir l'absence de tout conflit d'intérêt.

7.13(6) L'organisme de certification doit entreprendre et tenir à jour un registre des plaintes et appels. Ce registre doit inclure :

a) l'état d'avancement du traitement de chaque plainte ou appel (par exemple : reçue, en traitement, close, etc.) ;

b) les dates des actions réalisées (par exemple : accusé de réception, recevabilité, information du plaignant, réponse finale, sans suite, etc.).

8. Exigences du système de management

8.1 Généralités

8.1(1) En complément des exigences du §8 de l'ISO 17065, l'organisme de certification doit instaurer et maintenir un système de management à même de garantir le respect cohérent des exigences du présent référentiel pour la certification des prestataires de formation à la protection des données approuvée par la CNIL.

Cela implique que la mise en œuvre de ces exigences complémentaires doit être documentée, évaluée et surveillée de manière indépendante pour garantir la conformité, la transparence et le caractère vérifiable du respect des exigences du présent référentiel.

8.1(2) Les règles de fonctionnement du système de management et la documentation de sa mise en œuvre doivent être présentées par l'organisme de certification durant la procédure d'accréditation et accessible par la CNIL à sa demande.

8.2 Documentation générale du système de management

8.2(1) Les exigences du §8.2 de l'ISO 17065 s'appliquent.

8.3 Maîtrise des documents

8.3(1) Les exigences du §8.3 de l'ISO 17065 s'appliquent.

8.4 Maîtrise des enregistrements

8.4(1) Les exigences du §8.4 de l'ISO 17065 s'appliquent.

8.5 Revue de direction

8.5(1) Les exigences du §8.5 de l'ISO 17065 s'appliquent.

8.6 Audits internes

8.6(1) Les exigences du §8.6 de l'ISO 17065 s'appliquent.

8.7 Actions correctives

8.7(1) Les exigences du §8.7 de l'ISO 17065 s'appliquent.

8.8 Actions préventives

8.8(1) Les exigences du §8.8 de l'ISO 17065 s'appliquent.