# RÉFÉRENTIEL

## RELATIF AUX EXIGENCES D'AGRÉMENT DES ORGANISMES DE CERTIFICATION POUR LES MÉCANISMES DE CERTIFICATION APPROUVÉS AU TITRE DE L'ARTICLE 42 DU RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES




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 selon les critères d'un mécanisme de certification approuvés au titre de l'article 42 du règlement général sur la protection des données (RGPD).

## 2. Portée du référentiel

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

Il constitue le cadre général applicable pour la certification selon les mécanismes de certification approuvés au titre de l'article 42 du RGPD dès lors qu'il a été décidé, conformément à la convention de coopération conclue entre la CNIL et le Comité français d'accréditation (COFRAC), 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 43 du RGPD.

Ce cadre général peut être complété par des modalités d'application propres à un mécanisme de certification. Dans ce cas, des règles spécifiques à la mise en œuvre du mécanisme de certification précisent les exigences de ce référentiel pour l'évaluation des organismes certificateurs.
Ce référentiel n'est pas applicable dès lors que la CNIL décide de procéder à tout ou partie de l'agrément des organismes certificateurs.

## 3. Modalités d'accréditation

L'organisme de certification candidat dépose un dossier de demande d'accréditation auprès du COFRAC.

Ce dossier précise la portée de sa demande d'accréditation en indiquant le mécanisme de certification approuvé au titre de l'article 42 du RGPD pour lequel il souhaite délivrer des certifications.

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 il ait reçu une réponse favorable du COFRAC suite à la revue de sa demande d'accréditation, appelée recevabilité opérationnelle conformément au règlement d'accréditation du COFRAC.

Cette période transitoire ne peut excéder 12 mois : l'organisme de certification dispose d'une période 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 42 du RGPD.

## 4. Durée de l'agrément

La durée de l'agrément est celle de l'accréditation délivrée par le COFRAC.

## 5. Obligations de l'organisme de certification

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

(1) être mesure de démontrer au COFRAC sa conformité aux exigences définies en partie 6 de ce référentiel ;

(2) 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.

Il doit informer le COFRAC :

(3) s'il fait l'objet, ou a fait l'objet, d'un contrôle, d'une décision de sanction et/ou de mesures correctrices récentes prononcées par la CNIL ou par une autre autorité de contrôle compétente au sens du RGPD ;

(4) de toute autre décision contraignante qui pourrait constituer une non-conformité au présent référentiel, y compris les décisions d'autorités judiciaires compétentes ;

(5) dans le cas de changements significatifs de son statut juridique ou de toute autre situation affectant son activité qui serait susceptible de remettre en question sa conformité au présent référentiel ;

(6) d'autres changements avant leur mise en œuvre lorsque le mécanisme de certification introduit de nouvelles règles qui modifient substantiellement les conditions d'accréditation (p. ex. : des modifications substantielles relatives à la méthodologie d'évaluation) ou lorsque les critères du mécanisme de certification sont mis à jour.

Il doit informer la CNIL :

(7) avant de commencer à exploiter un label européen de protection des données approuvé par le Comité européen de la protection des données (CEPD) dans un nouvel État membre à partir d'un bureau satellite. Dans ce cas, l'organisme de certification doit également informer l'autorité de contrôle compétente de cet État membre.

Il est également soumis aux obligations suivantes :

(8) En cas de suspension de l'accréditation, il n'est plus autorisé à délivrer de certificats jusqu'à la levée de la suspension par le COFRAC. Pendant cette période, l'organisme de certification doit néanmoins poursuivre la surveillance des certifications en cours de validité ;

(9) 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 recevabilité de sa demande d'accréditation mais n'est pas parvenu à obtenir une accréditation auprès du COFRAC 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 organismes titulaires d'un certificat délivré par l'organisme de certification (organismes certifiés) ou en cours de certification. Ceux-ci choisissent un autre organisme certificateur accrédité ou en cours d'accréditation par le COFRAC pour transférer leur certification.

# 6. Exigences à satisfaire par les organismes de certification

**Référentiel d'évaluation**
**Mécanismes de certification approuvés au titre de l'article 42 du RGPD**
**Version du 22-09-2022**

## 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 les mécanismes de certification approuvés par la CNIL ou par le Comité européen de la protection des données (CEPD), conformément à l'article 42-5 et à l'article 43-2-b) du règlement général sur la protection des données (RGPD).

La nature des traitements de données à caractère personnel dans le champ d'application du mécanisme de certification (par exemple, une certification applicable aux traitements relatifs aux services en nuage) doit être pris en compte lors du processus d'accréditation de l'organisme de certification. Par exemple, cela inclut la prise en compte du type d'opérations de traitement de données auquel les critères de certification s'appliquent, les compétences appropriées pour la réalisation des activités de certification ou les méthodes d'évaluation pertinentes pour établir la conformité aux critères de certification.

À cette fin, un schéma de certification peut préciser les exigences de la norme EN ISO/IEC 17065 ou les exigences du présent référentiel, pour certains domaines d'application d'un mécanisme de certification. Les exigences du présent référentiel font référence aux règles qui peuvent être définies par le schéma de certification et qui s'imposent alors à l'organisme de certification dans le cadre de son accréditation.

## 2. Références normatives

EN ISO/IEC 17065:2012 : « 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 supplémentaires définies dans le présent référentiel ajoutent des spécificités liées à l'évaluation de traitements de données à caractère personnel mis en œuvre par un responsable de traitement ou un sous-traitant, conformément à l'article 43-1-b) du RGPD.

Le RGPD prévaut sur la norme ISO 17065. Toutefois, les exigences supplémentaires définies dans le présent référentiel ne peuvent contredire les règles concernant l'organisation et le fonctionnement de l'accréditation des organismes d'évaluation chargés d'accomplir des tâches d'évaluation de la conformité définie par le Règlement (CE) n°765/2008 du Parlement européen et du Conseil du 9 juillet 2008.

S'il est fait référence à d'autres normes ISO dans le schéma d'un mécanisme de certification approuvé par la CNIL ou par le CEPD, celles-ci sont interprétées conformément aux exigences définies par le RGPD.

| 3. Termes et définitions |
|---|
| Les termes et définitions des lignes directrices du CEPD relatives à l'agrément[1] et à la certification[2] s'appliquent. Ceux-ci complètent les termes et définitions de la norme EN ISO/IEC 17065:2012.<br>Afin de faciliter la lecture du présent référentiel, les principales définitions sont listées ci-après. |
| **RGPD** : Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (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 |
| **Mécanisme de certification** : outil de conformité permettant à un responsable de traitement ou un à sous-traitant d'obtenir une certification relative à ses opérations de traitement de données à caractère personnel |
| **Champ d'application du mécanisme de certification** : ensemble des opérations de traitement de données à caractère personnel qui répondent aux conditions d'éligibilité du mécanisme de certification |
| **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. Les critères de certification font l'objet d'une approbation par le CEPD ou par la CNIL (critères approuvés) |
| **Processus de certification** : ensemble des activités conduisant à la délivrance de la certification et au maintien de la validité de cette attestation (p. ex. : activité 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<br>Note 1 : les **audits internes** sont réalisés par, ou pour le compte de l'organisme lui-même.<br>Note 2 : les **audits de seconde partie** sont réalisés par des parties ayant un intérêt à l'égard de l'organisme, comme les clients ou d'autres personnes agissant en leur nom. |
| **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 opère un mécanisme de certification en réalisant les tâches du processus de certification |
| **Organisme apparenté :** organisme lié à l'organisme de certification, partiellement ou intégralement, par le biais d'actionnaires communs, partageant les mêmes membres au sein de leur conseil d'administration, des dispositions contractuelles, des dénominations communes, un |

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

| |
|---|
| personnel commun, des accords officieux ou autres ressources, de telle sorte que l'organisme apparenté est directement concerné par toute décision de certification ou possède la faculté d'influer sur le processus |
| **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 les mécanismes de certification approuvés au titre de l'article 42 du RGPD) |
| **Champ des activités de certification (ou portée d'agrément)** : activités réalisées par l'organisme de certification pour lesquelles celui-ci dispose d'un agrément |
| **Schéma de certification (ou programme de certification)** : ensemble des exigences, règles et procédures applicable à un mécanisme de certification. Le schéma de certification inclut les critères de certification, certaines règles relatives à l'application des exigences d'agrément et un ensemble de procédures applicables au processus de certification, notamment s'agissant de la mise en œuvre de la méthode d'évaluation |
| **Propriétaire du schéma de certification** : personne ou organisme responsable du développement et de la tenue à jour du schéma de certification |
| **Client (ou candidat)** : responsable de traitement ou sous-traitant qui a obtenu une certification ou qui en a fait la demande auprès d'un organisme de certification |
| **Objet de la certification (ou cible d'évaluation)** : ensemble d'opérations de traitement de données à caractère personnel, qui sont impliquées dans un produit, un procédé ou un service au sens de la norme ISO 17065, qu'un responsable de traitement ou un sous-traitant souhaite soumettre au processus de certification |
| **Périmètre de la certification** : ensemble d'activités réalisées par le client (ou le demandeur) qui impliquent l'objet de la certification. L'identification du périmètre de la certification permet à l'organisme de certification de déterminer le champ d'application du processus de certification (p. ex. : localisation géographique des activités, traitements sous-traités, etc.) |
| **Méthode d'évaluation** : procédure(s) mise(s) en œuvre par l'organisme de certification pour l'évaluation de l'objet de la certification |
| **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** : reconnaissance d'une certification existante et valide, qui est délivrée par un organisme de certification accrédité, par un autre organisme de certification accrédité, afin d'émettre sa propre certification |

## 4. Exigences générales

### 4.1 Domaine juridique et contractuel

#### 4.1.1 Responsabilité juridique

**4.1(1)** L'organisation de certification doit mettre en œuvre des procédures à jour tenant compte du régime de responsabilité auquel il est soumis au titre de ses missions telles que prévues dans les conditions d'agrément, incluant la conformité aux exigences supplémentaires du présent référentiel conformément à l'article 43-1-b) du RGPD.

En particulier, l'organisme de certification doit être en mesure de démontrer qu'il dispose de procédures et mesures conformes au RGPD en ce qui concerne spécifiquement le traitement des données à caractère personnel de son client dans le cadre du processus de certification.

#### 4.1.2 Contrat de certification (entre l'organisme de certification et ses clients)

**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 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 conformément à l'article 42-6 du RGPD, 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 du COFRAC à l'évaluation du client en tant qu'observateur ;

d) respecter les délais et les procédures applicables. Le contrat de certification doit mentionner que les délais et les procédures découlant, par exemple, du schéma de certification ou d'autres réglementations doivent être respectés ;

e) informer l'organisme de certification en cas de changements significatifs de sa situation légale ou de sa situation de fait, de changements significatifs des traitements de données dans le périmètre de la certification, de tout changement 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) ;

f) informer sans délai l'organisme de certification des manquements au RGPD ou à la loi Informatique et Libertés lorsqu'ils sont établis par la CNIL, ou par une autorité judiciaire, et qu'ils sont susceptibles de constituer une non-conformité aux critères de certification.

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

- les informations relatives à la délivrance et au retrait de la certification conformément aux exigences du §7.6 (Décision de certification) du présent référentiel ;

- sur demande de la CNIL, 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) des méthodes d'évaluation qui seront appliquées par l'organisme de certification pour l'examen de la cible d'évaluation, telles que prévues par l'exigence au §7.3(2) b) du présent référentiel ;

c) des mesures organisationnelles et des procédures mises en place par l'organisme de certification pour le besoin de la gestion des plaintes et des appels, conformément à l'article 43-2-d) du RGPD. 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 ;

d) des règles applicables au maintien de la certification, à son renouvellement, à sa suspension et à son retrait, conformément à l'article 42-7 du RGPD, y compris les règles relatives aux intervalles de surveillance et de réévaluation de la certification conformément aux exigences du §7.9 du présent référentiel ;

e) des conséquences générales d'une arrivée à terme de la période d'agrément, d'une suspension, d'un retrait ou d'une non-délivrance de celle-ci. 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 agrément pour un mécanisme de certification approuvé au titre de l'article 42.

### 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 un produit, un procédé ou un service certifié, en s'assurant que :

a) le mécanisme de certification est clairement mentionné et, lorsque cela s'applique, le sous-ensemble de critères applicable à la cible d'évaluation est indiqué. En particulier, la communication est transparente sur le type d'opérations de traitement couvert par les critères de certification lorsque le mécanisme de certification s'applique à un domaine spécifique ;

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

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

Note : Dans le cas d'un mécanisme de certification généraliste, il est possible que seul un sous-ensemble de critères s'applique à certaines cibles d'évaluation. Par exemple, lorsque le champ d'application du mécanisme de certification permet à la fois à des responsables de traitement et à des sous-traitants de candidater, la liste des critères qui s'appliqueront à la cible d'évaluation d'un responsable de traitement sera significativement différente de la liste des critères qui s'appliqueront lorsque les opérations de traitement des données à caractère personnel de la cible d'évaluation sont effectuées par un sous-traitant pour le compte d'un responsable du traitement.

**4.1.3(2)** L'usage incorrect ou ambigu de licences, certificats, marques de conformité, ainsi que tout autre dispositif destiné à identifier un produit, un procédé ou un service certifié doit être corrigé par une action appropriée. *A minima*, cela inclut :

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

b) l'obligation pour le 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 client ;

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 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 fournir des preuves :

a) de son indépendance conformément à l'article 43-2-a) du RGPD. Cela inclut des preuves concernant le financement de l'organisme de certification dans la mesure où l'assurance d'impartialité est concernée ;

b) que ses missions et ses obligations n'entraînent pas de conflit d'intérêts au sens de l'article 43-2-e) du RGPD ;

c) qu'il n'entretient pas de lien significatif avec les clients qu'il évalue.

Note : En complément des exigences du présent référentiel visant à prévenir le conflit d'intérêts, les exigences du §4.2 et §5.2 de l'ISO 17065, concernant la gestion des conflits d'intérêts identifiés, s'appliquent. En particulier, l'organisme de certification doit identifier régulièrement les risques susceptibles de nuire à son impartialité et doit prendre les mesures nécessaires lorsqu'il prend conscience que son impartialité est menacée par les actions d'autres personnes, entités ou organismes.

**4.2(2)** En particulier, l'organisme de certification doit s'assurer pour chacun de ses clients que :

a) le personnel impliqué dans les procédures d'évaluation, de revue et de prise de décision de certification n'a pas d'autre lien avec son client que son activité de certification et n'a pas d'activité en lien avec l'objet de la certification qui serait susceptible de remettre en cause l'impartialité de l'organisme de certification ;

b) son client n'est pas un organisme apparenté (ou une relation telle que définie au §4.2.3 de l'ISO 17065) qui présente un risque pour l'impartialité de l'organisme de certification ;

c) il n'a pas eu de relations économiques avec son client depuis au moins 2 ans (à l'exception de celles définies par un contrat de certification) et n'est pas financé par son client pour d'autres activités que la certification. En particulier, l'organisme de certification ne doit pas confier d'activités de traitement de données à caractère personnel à son client.

## 4.3 Responsabilité et financement

**4.3(1)** En complément des exigences du §4.3 de l'ISO 17065, l'organisme de certification doit prendre les mesures nécessaires (par exemple, assurances ou provisions) pour couvrir ses engagements dans les régions géographiques où il opère le mécanisme de certification.

## 4.4 Conditions non discriminatoires

**4.4(1)** En complément des exigences du §4.4 de l'ISO 17065, l'organisme de certification doit être transparent avec les candidats concernant :

a) les types de traitement de données qui sont le champ d'application du mécanisme de certification et qui sont également dans le champ de ses activités de certification (portée d'agrément).

En particulier, lorsque l'organisme de certification ne dispose pas d'une méthodologie d'évaluation adéquate pour l'évaluation de traitements de données pour un secteur d'activité (par exemple, lorsque l'évaluation implique le traitement de catégories particulières de données à caractère personnel ou l'utilisation de technologies particulières à un secteur) ou lorsque son personnel n'a pas les compétences appropriées pour évaluer un type de traitement de données, l'organisme de certification informe les candidats de ces limitations et fournit une liste des secteurs d'activité dans le champ de ses activités d'évaluation pour ce mécanisme de certification ;

b) la liste des États membres de l'Union européenne qui sont dans le champ de ses activités de certification, pour un mécanisme de certification transnational approuvé par plusieurs autorités de contrôle compétentes ou pour un label européen de protection des données approuvé par le CEPD.

En particulier, lorsque l'organisme de certification ne dispose pas d'une méthodologie d'évaluation adéquate pour l'évaluation de traitements de données soumis aux spécificités nationales d'une loi relative à la protection des données d'un État membre de l'Union européenne ou lorsque son personnel n'a pas les compétences appropriées pour évaluer les traitements dans le contexte de des

spécificités nationales d'un État membre, l'organisme de certification informe les candidats de ces limitations et fournit une liste des États membres de l'Union européenne dans le champ de ses activités d'évaluation pour ce mécanisme de certification.

### 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 à soumettre à la CNIL dans le cadre de l'annuaire des certifiés (voir les exigences du §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 lui transmettre 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), y compris des informations protégées par une confidentialité contractuelle qui sont liées au respect des règles en matière de protection des données.

En particulier, l'organisme de certification ne doit pas collecter d'informations confidentielles pour lesquelles le client pourrait légitimement invoquer les secrets opposables aux membres et agents de la CNIL dans l'exercice de leurs missions et strictement délimités à l'article 19-III de la loi Informatique et Libertés, à savoir : les informations couvertes par le secret professionnel applicable aux relations entre un avocat et son client, par le secret des sources des traitements journalistiques ou par le secret médical.

**4.5(3)** L'organisme de certification doit informer le client que la CNIL dispose du pouvoir de procéder à un examen des certifications délivrées en application de l'article 42-7 du RGPD. Les conditions applicables à l'exercice de ce pouvoir conféré à la CNIL en vertu de l'article 58 sont définies par le RGPD et la loi Informatique et Libertés et sont en dehors en champ d'application du présent référentiel.

### 4.6 Informations accessibles au public

**4.6(1)** En complément des exigences du §4.6 de l'ISO 17065, l'organisme de certification doit rendre accessible au public :

a) toutes les versions (courantes et précédentes) des critères de certification qui sont actuellement utilisées dans les certificats délivrés, en mentionnant leurs périodes de validité respectives ;

b) les versions obsolètes des critères de certification qui ne sont plus utilisées dans des certificats valides, en mentionnant leurs périodes de validité respectives ;

c) les procédures de certification actualisées, y compris les procédures de traitement des plaintes et des appels conformément à l'article 43-2-d) du RGPD ;

d) les informations sur la manière dont les procédures de certification sont concrètement mises en œuvre, notamment sur les moyens mis à la disposition des personnes concernées par les traitements de données à caractère personnel dans le périmètre de la certification pour faire une réclamation et sur la manière dont celle-ci sera traitée par l'organisme de certification.

## 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 dispose des compétences appropriées et actualisées (connaissances et expérience), conformément à l'article 43-1 du RGPD, pour mener à bien ses activités de certification. En particulier, le personnel doit :

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

b) disposer de connaissances et d'une expérience pertinente et appropriée en matière d'analyse et/ou de mise en œuvre de la réglementation applicable à la protection des données à caractère personnel (RGPD, la loi Informatique et Libertés et autres lois nationales applicables aux traitements de données dans le champ d'application du mécanisme de certification) ;

c) disposer de connaissances et d'une expérience pertinente et appropriée en matière d'analyse et/ou de mise en œuvre de mesures techniques et organisationnelles de protection des données dans le champ d'application du mécanisme de certification, conformément à l'article 43-2-a) du RGPD ;

d) disposer d'une expérience appropriée dans l'évaluation de traitements de données (audit).

Note : Le caractère 'pertinent' et 'approprié' des connaissances et de l'expérience du personnel doit être défini par l'organisme de certification de manière à ce que chaque personne intervenant dans le processus de certification (traitement de la demande, évaluation, revue, prise de décision, surveillance, etc.) soit capable de réaliser ses tâches, en prenant en compte des règles définies par le schéma de certification et dans le respect des exigences minimales définies par le présent référentiel quant aux compétences du personnel.

Cela inclut la prise en compte de besoins spécifiques en compétences liés au champ d'application du mécanisme de certification et/ou aux cibles d'évaluation qui peuvent être proposées à la certification, par exemple, pour des secteurs d'activités particuliers auxquels le mécanisme de certification s'applique (p. ex. : l'hébergement de données), certaines catégories de données à caractère personnel (p. ex. : les données de santé) ou encore des technologies spécifiques mises œuvre par certains services (p. ex. : technologie de traçage sur internet).

**6.1(2)** L'organisme de certification doit s'assurer que le personnel en charge des évaluations a :

a) suivi une formation relative aux méthodes d'évaluation (principes de l'audit, procédures et technique de l'audit, documentation relative à l'audit, règles et exigences applicables à l'audit, etc.) ;

b) pris part à au moins 2 audits complets, de la préparation de l'audit jusqu'aux conclusions finales, au cours des 3 dernières années.

Note : Les audits internes et les audits de seconde partie sont acceptés dès lors que l'évaluation a été réalisée sur la base d'exigences ou de règles internes établies et selon une procédure d'audit.

**6.1(3)** L'organisme de certification doit s'assurer que le personnel responsable de la revue et/ou de la prise de décision de certification dispose de connaissances approfondies et d'une expérience en matière de :

a) état de l'art, risques et enjeux an matière de protection des données à caractère personnel ;

b) mise en œuvre du processus de certification.

Note : Lorsque l'organisme de certification désigne une personne ou un groupe de personnes pour prendre une décision de certification conformément au §7.6.2 de l'ISO 17065 et si ce personnel ne dispose pas des connaissances ou de l'expérience requise au 6.1(3) du présent référentiel, le processus de certification conduisant à cette décision de certification individuelle doit inclure un processus de

revue de la certification qui implique au moins une personne disposant des compétences requises par l'exigence au §6.1(3) du présent référentiel.

**6.1(4)** L'organisme de certification doit disposer de personnel avec une expertise technique et une expertise juridique dont les profils répondent :

a) aux exigences relatives au profil d'expertise technique, telles que définies au §6.1(5), §6.1(6) et §6.1(7) du présent référentiel ;

b) aux exigences relatives au profil d'expertise juridique, telles que définies au §6.1(8) et §6.1(9) du présent référentiel.

Note : Les périodes de stages et d'apprentissage ne constituent pas une expérience de travail prise en compte pour attester du nombre d'années d'expérience professionnelle requise pour le personnel chargé de l'évaluation ou de la revue de la certification, telle que fixée par le présent référentiel.

**6.1(5)** (Profil d'expertise technique) L'organisme de certification doit s'assurer que le personnel disposant d'une expertise technique justifie :

a) *a minima* d'un diplôme de niveau licence, ou correspondant au moins au niveau EQF6[3] du cadre européen des certifications, dans le domaine de l'informatique, des systèmes d'information ou de la cybersécurité ou bien d'un titre reconnu par l'État (p. ex. : diplôme d'Ingénieur) dans ces domaines ;

b) ou dispose d'une expérience professionnelle significative d'au moins 5 années dans le domaine de la protection des données.

Note : L'expérience professionnelle requise au §6.1(5) b) du présent référentiel constitue une alternative au diplôme requis au §6.1(5) a) (« Validation des Acquis de l'Expérience – VAE » dans le contexte de ce référentiel). Cette même expérience professionnelle peut également être prise en compte, lorsqu'elle est appropriée, pour répondre aux autres exigences d'expérience professionnelle du présent référentiel.

**6.1(6)** (Profil d'expertise technique) L'organisme de certification doit s'assurer que son personnel disposant d'une expertise technique a suivi une formation d'au moins 2 jours *a minima* sur les référentiels utiles au management de la sécurité des systèmes d'information (réglementation, normes, méthodes, bonnes pratiques, gestion des risques, etc.).

**6.1(7)** (Profil d'expertise technique) L'organisme de certification doit s'assurer que son personnel au profil d'expertise technique dispose de compétences appropriées et actualisées qui incluent :

a) pour le personnel en charge de l'évaluation, une expérience de 2 ans *a minima* dans le domaine de la protection des données, telle que l'analyse et/ou la mise en œuvre de mesures techniques et organisationnelles de sécurisation des systèmes d'information et qui est adaptée au champ d'application du mécanisme de certification (p. ex. : tests de mesures de sécurité des données, procédures d'évaluation ou de certifications techniques) ;

b) pour le personnel responsable de la revue de la certification (ou de la prise de décision), une expérience de 2 ans *a minima* dans l'identification, la définition, la surveillance de mesures de protection des données ou dans une activité de conseil en matière de protection des données.

**6.1(8)** (Profil d'expertise juridique) L'organisme de certification doit s'assurer que son personnel disposant d'une expertise juridique justifie :

a) *a minima* d'un diplôme de niveau master 1 dans le domaine du droit ou d'un diplôme reconnu par un État membre de l'Union européenne, correspondant à au moins 8 semestres et ayant débouché à un diplôme universitaire équivalent (maîtrise en droit) ;

b) ou dispose d'une expérience professionnelle significative d'au moins 5 années dans le domaine de la protection des données à caractère personnel.

[3] https://europa.eu/europass/en/european-qualifications-framework-eqf

Note : L'expérience professionnelle requise au §6.1(8) b) du présent référentiel constitue une alternative au diplôme requis au §6.1(8) a) (« Validation des Acquis de l'Expérience – VAE » dans le contexte de ce référentiel). Cette même expérience professionnelle peut également être prise en compte, lorsqu'elle est appropriée, pour répondre aux autres exigences d'expérience professionnelle du présent référentiel.

**6.1(9)** (Profil d'expertise juridique) L'organisme de certification doit s'assurer que son personnel au profil d'expertise juridique dispose de compétences appropriées et actualisées qui incluent :

a) pour le personnel en charge de l'évaluation, une expérience de 2 ans *a minima* dans le domaine du droit de la protection des données, telle que l'analyse et/ou la mise en œuvre de la conformité à la réglementation applicable aux traitements des données à caractère personnel (p. ex. : revue de contrats ou procédure d'évaluation relative aux droits des personnes concernées) ;

b) pour le personnel responsable de la revue de la certification (ou de la prise de décision), une expérience de 2 ans *a minima* dans la surveillance de la conformité de mesures de protection des données ou dans une activité de conseil en matière de protection des données à caractère personnel.

**6.1(10)** L'organisme de certification doit s'assurer du maintien des compétences de son personnel, par exemple au moyen d'un programme de formation professionnelle.

**6.1(11)** En complément des exigences du §6.1.3 de l'ISO 17065, l'organisme de certification doit exiger de son personnel participant au processus de certification qu'il s'engage à respecter les règles définies par l'organisme de certification s'agissant de l'indépendance du personnel d'intérêt commerciaux ou autres concernant l'objet de certification conformément à l'article 43-2-a) du RGPD.

L'organisme de certification doit utiliser ces informations comme données d'entrée pour identifier les risques que font peser sur l'impartialité les activités de ce personnel ou des organismes qui les emploient conformément aux exigences du §4.2.3 de l'ISO 17065 et démontrer que leurs missions n'entraînent pas de conflit d'intérêts conformément à l'article 43-2-e) du RGPD.

### 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.

Conformément aux exigences du §6.2.2.4 et du §7.6.1 de l'ISO 17065, l'organisme de certification doit assumer l'entière responsabilité de toutes les activités externalisées auprès d'un autre organisme et il doit être responsable et doit conserver son pouvoir décisionnel en matière de certification.

**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 personne en charge de l'évaluation, 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 client que le processus de certification et n'a pas d'activité en lien avec l'activité du client 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 opérations de traitement des données à caractère personnel doivent être évaluées selon les critères de certification approuvé par la CNIL au titre de l'article 58-3 du RGPD et d'article 8-I-2°-h) de la loi Informatique et Libertés ou par le CEPD au titre de l'article 63 du RGPD.

Note : Pour réaliser son évaluation, l'organisme de certification peut prendre en compte les guides ainsi que les méthodes d'évaluation ou de tests fournies par le propriétaire du schéma de certification.

### 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 candidat les informations suivantes en rapport avec l'objet de la certification :

a) une description détaillée de la cible d'évaluation, comprenant ses interfaces avec d'autres systèmes et/ou organisations. En particulier, les protocoles sous-jacents et les garanties liées à ces interfaces d'échange, qui permettent la communication de données entre la cible d'évaluation et des systèmes externes et/ou des organisation tierces, sont fournis ;

b) la liste des transferts de données à des organisations situées dans un pays tiers (hors de l'Union européenne) ou vers une organisation internationale. Les réglementations nationales applicables à l'importateur des données et le type des garanties appropriées mises en œuvre sont indiquées ;

c) les responsabilités, activités de traitement et/ou rôle du candidat, lorsque le candidat est un sous-traitant ou un responsable de traitement conjoint ;

d) la liste des sous-traitants (ou des sous-traitants ultérieurs lorsque le candidat est lui-même sous-traitant). Leurs responsabilités et leurs activités de traitement doivent être décrites et les principaux contrats ou contrats-type liant le candidat à ses sous-traitant doivent être identifiés ;

e) la liste des responsables de traitement conjoints. Leurs responsabilités et rôles sont décrits et les principes de l'accord les liant avec le candidat doivent être indiqués (ou la nature de l'instrument juridique utilisé) ;

f) les caractéristiques générales des traitements de données dans le périmètre de la certification, telles que l'adresse des locaux du candidat où les données à caractère personnel sont traitées, les catégories de données impliquées et les obligations nationales qui s'appliquent aux traitements de données ;

g) le cas échéant, les informations relatives aux certifications ou à des résultats d'évaluation obtenues avant la demande de certification, lorsque la nature de ces évaluations et leur périmètre sont pertinents pour une éventuelle prise en compte dans le processus de certification ;

h) l'existence de toute action de contrôle en cours, ou décision de sanction et/ou de mesures correctrices récente prononcée par la CNIL ou par une autre autorité de contrôle compétentes à l'encontre du candidat, lorsqu'elle porte sur des traitements de données dans le périmètre de la certification demandée.

### 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 :

a) que l'objet de la certification est éligible à l'évaluation selon les critères de certification, en prenant en compte les règles définies par le schéma de certification. En particulier, l'organisme de certification doit s'assurer que le candidat et les opérations de traitement de données qu'il souhaite soumettre à l'évaluation sont dans le champ d'application du mécanisme de certification s'agissant :

- des responsabilités du candidat pour l'objet de certification proposé, compte-tenu de la réglementation applicable en matière de protection des données (responsable de traitement, responsable de traitement conjoint, sous-traitant, sous-traitant ultérieur, etc.) ;

- du type d'opérations de traitement de données de l'objet de certification, compte-tenu des opérations de traitement de données pour lesquels les critères de certification ont été conçus et approuvés au titre de l'article 42 du RGPD ;

b) qu'il dispose des méthodes d'évaluation adaptées à la cible d'évaluation, en prenant en compte :

- les règles définies par le schéma de certification concernant les méthodes à appliquer pour l'évaluation de la conformité des opérations de traitement de données aux critères de certification ;

- les réglementations applicables à la cible d'évaluation en matière de protection des données ;

- les actions de contrôle en cours ou les décisions de sanction et/ou mesures correctrices récentes prononcées par la CNIL ou d'autres autorités de contrôle compétentes ;

L'organisme de certification décrit les méthodes d'évaluation utilisées pour l'évaluation la conformité des opérations de traitement aux critères de certification de manière uniforme, en veillant à ce que des méthodes d'évaluation comparables soient utilisées pour l'évaluation de cibles d'évaluation comparables et concluent à des résultats comparables ;

c) qu'il possède les compétences juridiques et techniques nécessaires en matière de protection des données, conformément aux exigences du §6 du présent référentiel, pour réaliser l'activité de certification, en particulier lorsque l'organisme de certification ne dispose pas d'expérience ultérieure d'évaluation du même type d'objet de certification ou d'un périmètre de certification similaire.

**7.3(3)** Lorsque le schéma de certification définit des règles pour le calcul de la durée de l'activité d'évaluation (p. ex. : en jours), l'organisme de certification doit mettre en place une procédure de calcul de la durée d'audit. Pour l'application de la méthode d'évaluation, cette procédure doit prendre en compte les facteurs suivants :

a) l'ampleur des traitements de données à caractère personnel dans le périmètre de certification ;

b) la nature des données à caractère personnel traitées ;

c) les risques pour les personnes concernées par les traitements de données ;

d) la complexité de l'évaluation des technologies utilisées pour les traitements de données ;

e) le recours à des sous-traitants pour réaliser les traitements de données ;

f) le nombre de structures/établissements du candidat dans lesquels sont effectués les traitements de données à caractère personnel.

Lorsque le schéma de certification définit des règles pour le calcul d'une durée (minimale) d'évaluation du client, l'organisme de certification doit réaliser ce calcul selon les règles définies par le schéma de certification et déterminer si la durée calculée est suffisante pour réaliser ses tâches d'évaluation ou si cette durée doit être augmentée. Il conserve la justification et un enregistrement de la durée retenue.

La durée d'audit retenue par l'organisme de certification est indiquée dans le contrat de certification.

**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 suit les règles définies par le schéma de certification qui s'appliquent.

En particulier, 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 de la cible d'évaluation 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). Le plan d'audit doit permettre la mise en œuvre la méthode d'évaluation établie dans le contrat de certification, conformément à l'exigence §4.1.2(2) b) du présent référentiel.

La mise en œuvre de la méthode d'évaluation peut nécessiter une évaluation dans les locaux du client afin de réaliser les constatations nécessaires pour établir la conformité aux critères de certification. Tout écart à la méthode d'évaluation doit être justifié par l'organisme de certification.

**7.4(2)** L'organisme de certification doit appliquer les méthodes d'évaluation établies dans le contrat de certification lors de son évaluation, par exemple en appliquant :

a) une méthode pour l'évaluation de la nécessité et de la proportionnalité des opérations de traitement de données au regard de l'objectif poursuivi et de la sauvegarde des droits fondamentaux et des intérêts de la personne concernée ;

b) une méthode pour l'évaluation de l'étendue, le type et l'appréciation de l'ensemble des risques envisagés par le responsable de traitement et le sous-traitant s'agissant de leurs obligations conformément aux article 30, 32, 35 et 36 du RGPD, et du caractère approprié des mesures techniques et organisationnelles prévues aux articles 24, 25 et 32 du RGPD, dans la mesure où les articles susmentionnés s'appliquent à l'objet de la certification ;

c) une méthode pour l'évaluation des actions correctives, y compris les garanties, mesures de sauvegarde et procédures permettant d'assurer la protection des données à caractère personnel pour les traitements de données impliqués dans la cible d'évaluation.

**7.4(3)** L'organisme de certification doit désigner du personnel avec des compétences appropriées pour effectuer les tâches d'évaluation, en prenant en compte les règles définies par le schéma de certification. L'organisme de certification s'assure que le personnel impliqué dans les tâches d'évaluation de la certification, que ces ressources soient internes à l'organisme ou externes, répond aux exigences de compétences, telles que spécifiées au §6 du présent référentiel.

En particulier, pour chaque évaluation, l'organisme de certification s'assure que l'équipe en charge de l'évaluation, dans son ensemble, dispose des compétences juridiques et techniques telles que définies au §6 du présent référentiel.

De manière exceptionnelle, lorsque l'organisme de certification fait intervenir en évaluation une personne qui ne peut justifier de compétences répondant aux exigences de qualification en tant que « profil technique » ou au « profil juridique », telles que définies au §6 du présent référentiel, il justifie le besoin particulier de l'intervention d'un « expert » aux compétences spécifiques pour réaliser l'évaluation (p. ex. : une personne spécialisée dans une technologie particulière, dans un secteur d'activité impliquant le traitement de catégories particulières de données ou pour lequel des réglementations nationales sont applicables). Dans ce cas, le résultat des tâches d'évaluation conduites par la personne avec un profil « expert » doit faire l'objet d'une supervision, pendant le processus d'évaluation, par un membre du personnel en charge de l'évaluation et qui répond aux exigences de qualification en tant que « profil technique » ou « profil juridique » (p. ex. : le responsable de l'équipe d'audit).

**7.4(4)** En complément des exigences du §7.4.5 de l'ISO 17065 et 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 obtenue avant son évaluation, l'organisme de certification doit :

a) s'assurer que le certificat sera valide au moment de l'évaluation et que la certification obtenue est pertinente pour la cible d'évaluation ;

b) documenter comment et dans quelle mesure les résultats de la certification préalablement obtenue peuvent être pris en compte pour l'évaluation des critères de certification, dans le respect des règles définies par le schéma de certification ;

c) établir les conséquences pour l'évaluation restant à réaliser et sur la méthode d'évaluation à appliquer, par exemple en définissant une matrice de correspondance entre les critères des deux mécanismes de certification pour le contexte de la cible d'évaluation.

**7.4(5)** Lorsqu'il prend la responsabilité de s'appuyer sur des résultats d'une certification obtenue avant la demande de certification, l'organisme de certification doit s'assurer de la conformité de la cible d'évaluation à tous les critères du mécanisme de certification approuvé. En particulier, l'organisme de certification doit :

a) avoir accès à la totalité du rapport d'évaluation de la certification préalablement obtenue (et pas uniquement au certificat de conformité ou à une attestation similaire) ;

b) documenter ses propres constats en :

- faisant référence aux résultats pertinents du rapport d'évaluation préexistant (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 mécanisme de certification approuvé.

Si des écarts par rapport aux constats du rapport d'évaluation de la certification préalablement obtenue sont identifiés par l'organisme de certification lors de son évaluation des critères du mécanisme de certification approuvé, l'évaluation est étendue aux critères de certification concernés et, si nécessaire, pour la totalité de la cible d'évaluation déjà certifiée.

**7.4(6)** En complément des exigences du §7.4.6 de l'ISO 17065, l'organisme de certification doit définir dans ses procédures la manière dont le client est informé des résultats de l'évaluation, y compris des non-conformités, en prenant en compte les règles définies par le schéma de certification, notamment s'agissant de la forme de ces informations et du moment où elles sont fournies au client.

**7.4(7)** En complément des exigences du §7.4.9 de l'ISO 17065, l'organisme de certification doit documenter ses constats, pour chaque critère de certification, conformément aux règles définies par le schéma de certification. *A minima*, le rapport d'évaluation comprend :

a) la description de la cible d'évaluation ;

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

c) les références aux documents et enregistrements examinés ;

d) les références aux traitements de données à caractère personnel qui ont été évalués ;

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

f) les sites physiques du candidat où ont été réalisées les constatations ;

g) 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 son client 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(8)** 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, fichiers de journalisation, 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.

**7.4(9)** Si les données à caractère personnel du périmètre de certification sont traitées à partir de plusieurs structures/établissement du candidat, l'évaluation doit être effectuée selon les règles définies par le schéma de certification.

Lorsqu'une non-conformité est détectée pour l'une de ces structures/établissements, l'organisme de certification sollicite son client afin :

- qu'il en analyse l'étendue et les causes ; et

- qu'il propose la mise en œuvre de mesures visant à prévenir que cette non-conformité ne se reproduise dans d'autres localisations.

Ces analyses sont jointes au plan d'actions et examinées par l'organisme de certification.

### 7.5 Revue des résultats relatifs à l'évaluation

**7.5(1)** Conformément aux exigences du §7.5 de l'ISO 17065, l'organisme de certification effectue une revue de toutes les informations et de tous les résultats suite à l'évaluation.

En complément des exigences du §7.5 de l'ISO 17065, le processus de revue de l'évaluation doit prendre en compte les règles définies par le schéma de certification. En particulier, l'organisme de certification doit :

a) vérifier que le périmètre de la certification est cohérent avec l'objet de la certification qui a été l'évalué ;

b) vérifier que les méthodes d'évaluation ont été suivies et que les constatations disponibles dans le rapport d'évaluation sont pertinentes.

**7.5(2)** L'organisme de certification doit désigner du personnel avec des compétences appropriées pour effectuer la revue de la certification, en prenant en compte les règles définies par le schéma de certification. L'organisme de certification s'assure que le personnel impliqué dans la revue de la certification, que ces ressources soient internes à l'organisme ou externes, répond aux exigences de compétences, telles que spécifiées au §6 du présent référentiel.

En particulier, pour chaque revue, l'organisme de certification s'assure que le personnel en charge de la revue de l'évaluation dispose des compétences juridiques et techniques telle que définies au §6 du présent référentiel.

### 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, en prenant en compte les règles définies par le schéma de certification.

L'organisme de certification définit également des procédures pour prendre d'autres décisions relative 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 mise à jour du périmètre de certification (extension ou réduction du périmètre), la suspension ou la levée d'une suspension et 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 ;

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

d) en complément de la revue des informations réalisée au stade de la demande de certification (voir les exigences du §7.2(1) h) du présent référentiel), au sujet d'une action de contrôle en cours, ou d'une décision de sanction et/ou de mesures correctrices récente prononcée par la CNIL ou d'autres autorités de contrôle compétentes, l'organisme de certification vérifie avec le client que cette information est à jour avant de prendre une décision.

Si de nouveaux contrôles ont été réalisés auprès du client ou si des mesures correctrices ont été demandées, l'organisme de certification évalue si cela peut constituer une non-conformité aux critères de certification et empêcher la certification d'être délivrée (ou renouvelée, rétablie ou étendue).

L'organisme de certification documente dans son rapport d'évaluation (et/ou dans sa décision de certification) ses conclusions concernant les actions de contrôle ou les mesures correctrices demandées portant sur des traitements de données dans le périmètre de la certification ;

e) l'organisme de certification informe la CNIL de ses décisions, par écrit et avant l'application de sa décision, lorsque la certification est délivrée (renouvelée, rétablie ou étendue) ou retirée (réduite ou suspendue) conformément à l'article 43-5 du RGPD ;

L'information fournie à la CNIL doit inclure :

- le nom du client ;

- le périmètre de la certification ;

- la description de l'objet de la certification ;

- une synthèse du rapport d'évaluation qui explique en quoi les critères de certification sont satisfaits (ou pourquoi ils ne sont plus satisfaits) ;

- la documentation de certification officielle, telle que prévue au §7.7 du présent référentiel (le certificat émis) ;

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

**7.6(2)** L'organisme de certification doit définir ses procédures de certification de manière à garantir son indépendance et assumer ses responsabilités via à vis de ses décisions de certification. En particulier, l'organisme de certification doit démontrer que la ou les personnes qu'il missionne pour rendre 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 client des documents de certification officiels (certificat) qui permettent d'identifier :

a) le nom et la référence (y compris la version) des critères de certification qui ont été utilisées pour l'évaluation ;

b) le périmètre de la certification, qui inclut une description claire et compréhensible de l'objet de la certification et la liste des localisations du client où les données à caractère personnel sont traitées ;

Lorsque l'applicabilité d'un sous-ensemble des critères de certification dépend du contexte des opérations de traitement dans le périmètre de certification (p. ex. : le statut de responsable de traitement ou de sous-traitant, le traitement de catégories particulières de données, l'utilisation de technologies spécifiques, l'application des secteurs spécifiques d'activités, etc.), le périmètre de la certification doit être décrit de manière à ce que le sous-ensemble des critères qui ont été évalués soit compréhensible ;

c) l'objet de la certification (la cible d'évaluation), y compris la version ou autres éléments d'identification applicables.

**7.7(2)** L'organisme de certification fournit à son client une documentation de certification officielle (certificat) où la date d'échéance ou d'expiration de la certification est fixée conformément à la période de validité de la certification définie par le schéma de certification. L'organisme de certification s'assure que la période de validité de la certification ne dépasse pas 3 ans.

## 7.8 Annuaires des produits 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 cibles d'évaluation certifiées, conformément aux règles définies par le schéma de certification, comportant au moins :

a) le périmètre de la certification ;

b) une description claire et compréhensible de l'objet de la certification (une description pertinente de la cible d'évaluation), y compris la version or autres éléments d'identification applicables ;

c) le nom et/ou une référence (y compris la version) des critères de certification qui ont été utilisés pour l'évaluation ;

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

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

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

g) 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 comprennent un historique des actions réalisées par l'organisme de certification pour chaque cible d'évaluation certifiée. Elles n'ont pas à être rendues publiques, à moins que le schéma de certification stipule qu'elles doivent être publiées, contrairement aux informations prévues à l'exigence 7.8(2) du présent référentiel qui visent à rendre accessible au public la liste des cibles d'évaluation qui disposent d'un certificat valide. Elles doivent néanmoins être accessibles sur demande d'un tiers qui souhaite s'assurer du statut de validité d'une certification donnée, par exemple, pour une période antérieure déterminée ou bien pour une cible d'évaluation qui a connu des changements au cours du temps.

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

**7.8(2)** L'organisme de certification doit mettre à disposition du public une synthèse de la documentation relative à sa décision de certification de manière à favoriser la transparence concernant ce qui a été évalué et les méthodes d'évaluation utilisées. L'information à publier est définie par le schéma de certification.

L'organisme de certification doit, *a minima*, publier dans un annuaire une synthèse qui inclut :

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

b) le périmètre de la certification, qui inclut une description claire et compréhensible de l'objet de la certification ;

c) l'objet de la certification (la cible d'évaluation), y compris la version or autres éléments d'identification applicables ;

d) le nom et/ou une référence (y compris la version) des critères de certification qui ont été utilisés pour l'évaluation et, lorsque c'est le cas, les spécificités de la méthode appliquée pour évaluer la conformité des opérations de traitement de données aux critères de certification ;

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

f) 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. Le périmètre de la certification et l'objet de la certification doivent être fournis à la CNIL en langue française.

### 7.9 Surveillance et renouvellement

**7.9(1)** L'organisme de certification doit définir une procédure de surveillance de la conformité des cibles d'évaluation certifiées aux critères de certification, conformément à l'article 43-2-c) du RGPD.

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

a) une évaluation des changements qui ont été appliqués aux traitements de données concernés par le périmètre de la certification 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 que certaines opérations de traitement de données n'avaient pas encore démarré ;

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 (p. ex. : dossiers, contrats, interviews, etc.) afin de consolider les constats déjà établis ;

- l'analyse des enregistrement 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 nouvelles opérations de traitement dans le périmètre de la certification depuis la précédente évaluation ;

- l'analyse des traitements de données dans différents contextes du périmètre de la certification (p. ex. : évaluation dans d'autres localisations du client, de certains services ou processus personnalisés, etc.) afin de s'assurer que les constats établis sont cohérents.

**7.9(2)** L'organisme de certification doit planifier son activité de surveillance selon les règles définies par le schéma de certification. La période maximale entre les mesures de surveillance ne devrait pas excéder 12 mois.

En complément de ces 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 (p. ex. : description de la cible d'évaluation, etc.) ;

b) l'organisation d'une évaluation complémentaire à l'initiative de l'organisme de certification, lorsque cela est proportionné au risque en matière de protection des données à caractère personnel. 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(3)** 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 réduction du périmètre de certification, 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(4)** 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.

L'organisme de certification doit suivre les règles spécifiques définies par le schéma de certification qui s'appliquent au renouvellement de la certification. En particulier, ces règles peuvent concerner la délivrance du certificat (p. ex. : date d'effet du renouvellement de la certification).

**7.9(5)** Lorsque le client possède plusieurs structures/établissements, l'organisme de certification doit suivre les règles applicables définies par le schéma de certification, notamment s'agissant des conséquences sur le processus de certification de l'ajout (extension du périmètre) ou la résiliation de localisation (réduction du périmètre).

En particulier, l'organisme de certification planifie l'évaluation des sites du client sur la durée de validité de la certification.

## 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 manquement au RGPD ou à la loi Informatique et Libertés rapporté par le client à l'organisme de certification lorsqu'il est en lien avec l'objet de la certification ;

b) tout changement dans le traitement des données à caractère personnel indiqué par le client comme étant susceptible d'avoir des effets sur la conformité de l'objet de la certification aux critères de certification ;

c) toute modification apportée à la réglementation relative à la protection des données à caractère personnel lorsqu'elle concerne le champ d'application du mécanisme de certification ;

d) l'adoption d'actes délégués par la Commission européenne conformément à l'article 43-8 et 43-9 du RGPD en lien avec le champ d'application du mécanisme de certification ;

e) les décisions ou avis contraignants du CEPD et/ou de la CNIL en lien avec le champ d'application du mécanisme de certification ;

f) les décisions de justice en matière de protection des données à caractère personnel portées à sa connaissance en lien avec le champ d'application du mécanisme de certification ;

g) les nouveaux développements de l'état de l'art en matière de technologies utilisées pour le traitement de données à caractère personnel ;

h) les risques émergents en matière de protection des données.

Note : L'organisme de certification peut également prendre en compte les recommandations, bonnes pratiques et autres documents adoptés par le CEPD et/ou la CNIL en lien avec le champ d'application du mécanisme de certification.

**7.10(2)** L'organisme de certification doit définir une procédure de gestion lui permettant d'analyser, décider et mettre en œuvre les changements ayant des conséquences sur le processus de certification, en prenant en compte les règles définies par le schéma de certification. *A minima*, cette procédure inclut les points suivants :

a) établir et mettre à jour un registre répertoriant les changements analysés comme ayant des conséquences sur le processus de certification ainsi que les cibles d'évaluation impactées ;

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

- l'évaluation complémentaire ou la réévaluation immédiate des critères de certification ;

- les motifs qui ont conduit à ne pas réaliser immédiatement une évaluation complémentaire ou une réévaluation des critères de certification pour les cibles d'évaluation impactées ;

- 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 le propriétaire du schéma de certification à l'occasion d'une mise à jour des critères de certification, les délais applicables aux changements à mettre en œuvre et les conditions pour maintenir ou renouveler la certification pour les cibles d'évaluation impactées ;

c) informer le client, 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 les traitements des données dans le périmètre de la certification demeurent en conformité avec les critères de certification. L'évaluation planifiée doit être proportionnée aux conséquences sur la certification. Lorsqu'une période de transition est définie, le client 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 les traitements de données dans le périmètre de la certification ne sont plus conformes aux critères de certification ;

e) mettre à jour ses procédures de certification, y compris les méthodes d'évaluation impactées en prenant en compte les règles définies par le schéma de certification, de manière à ce qu'elles s'appliquent aux futurs clients de manière uniforme.

**7.10(3)** Dans le cas où le client informe l'organisme de certification d'une action de contrôle en cours, ou d'une décision de sanction et/ou de mesures correctrices récentes prononcées par la CNIL ou une autre autorité de contrôle, qui met en question la conformité du client aux règles de protection des données à caractère personnel, l'organisme de certification documente le résultat de son analyse s'agissant de savoir si la cible d'évaluation demeure en conformité avec les critères de certification, y compris ses conséquences lorsque l'évaluation aboutit à une décision de certification.

### 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 de la cible d'évaluation selon les règles définies par le schéma de certification. *A minima*, cette procédure inclut les points suivants :

a) lorsqu'une non-conformité aux critères de certification est avérée, l'organisme de certification doit déterminer si les actions correctives proposées par le client 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 clients 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 permet de garantir la conformité des opérations de traitement 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 ;

c) lorsque la certification du client 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'une évaluation complémentaire.

**7.11(2)** Lorsque la certification est résiliée à la demande du client, 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 ou lorsque le périmètre de la certification est réduit, l'organisme de certification informe la CNIL par écrit 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 client 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 doit conserver 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 client 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 des §7.4(8) et 7.9(3) du présent référentiel). Une traduction en langue française d'une partie de cette documentation doit être communiquée à la CNIL à sa demande.

### 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, en tant compte des règles définies par le schéma 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 ou du requérant quant aux suites données à sa plainte ou son appel ;

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 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 concernées par les traitements de données à caractère personnel dans le périmètre de la certification.

**7.13(4)** L'organisme de certification informe le plaignant ou le requérant de l'avancée du traitement et des suites données à sa demande 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 les mécanismes de certification dans la portée de son agrément.

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.

À cette fin, le système de management doit définir une méthodologie visant à satisfaire ces exigences complémentaires et à les contrôler, en conformité avec la réglementation relative à la protection des données, et à constamment les vérifier.

En particulier, le système de management doit garantir le respect des exigences au §4.6 (Informations accessibles au public) and §7.8 (Annuaires des produits certifiés) du présent référentiel, de manière à ce que soient rendues publiques, de façon permanente et continue, quelles sont les certifications qui ont été effectuées, sur quelle base (ou selon quels mécanismes de certification ou schéma de certification), quelle est la durée de validité des certifications et dans quel cadre et dans quelles conditions (considérant 100 du RGPD).

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

### 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. |
| **9. Autres exigences supplémentaires** |
| **9.1 Mise à jour des méthodes d'évaluation** |
| **9.1(1)** L'organisme de certification établit des procédures destinées mettre à jour les méthodes d'évaluation qui doivent être appliquées au §7.4 du présent référentiel. En particulier, cette mise à jour doit être envisagée sur la base des changements ayant des conséquences sur la certification (voir exigences du §7.10 du présent référentiel) et en tant que qu'action préventive telle que prévue au §8.8 de l'ISO 17065. |

# 7. Règles d'application spécifiques au mécanisme de certification

Des règles d'application spécifiques au mécanisme de certification et qui s'imposent à l'organisme de certification dans le cadre de son agrément peuvent être définies par le schéma du mécanisme de certification approuvé au titre de l'article 42 du RGPD.