REFERENTIEL DE CERTIFICATION

Certification des prestataires de formation à la protection des données à caractère personnel

Référentiel de certification
AC-REF-014-01 Ed. 3

Version du 11/04/2024

Tél : 01 45 66 18 18
RCS Nanterre 500 229 398 – SIRET : 500 229 398 00028 – APE : 7120B

Rédacteur : S.BELATRECHE Responsable Développement	Vérificateur : V.LIMOUSIN Responsable Qualité	Approbateur : P.LABROUSSE Directeur

Validation workflow documentaire ISAC

Sommaire

1. Contexte et domaine d'application

1.1. Contexte

La certification des prestataires de formation à la protection des données à caractère personnel est une certification basée sur le référentiel de la CNIL. Il s'agit d'un mécanisme volontaire permettant aux organismes de formation de justifier que leur prestation s'inscrit dans une logique de conformité au RGPD et à la loi Informatique et Libertés. Il concerne les prestataires de formation qui souhaitent valoriser le contenu de leur formation en protection des données personnelles, en vue de démontrer leur conformité avec les exigences de la CNIL.

Son objectif est d'attester de la qualité des actions des prestataires de formation en protection des données à caractère personnel sous un référentiel unique.

1.2. Domaine d'application

Le référentiel de la CNIL, paru en décembre 2020, énonce l'ensemble des critères d'obtention de la certification, auxquels le prestataire de formation devra démontrer sa conformité pour obtenir la certification. Ces critères sont répartis en 8 thématiques :

1. Exigences générales ;
2. Exigences relatives à l'information du public sur les formations proposées ;
3. Exigences relatives à l'identification des besoins et des objectifs de formation ;
4. Exigences relatives à la conception des formations
5. Exigences relatives à la préparation et à l'adaptation des formations aux apprenants
6. Exigences relatives aux conditions de réalisation des formations;
7. Exigences relatives aux compétences des intervenants ;
8. Exigences relatives au recueil des appréciations et la prise en compte des réclamations.

Le programme de certification « certification des prestataires de formation à la protection des données à caractère personnel » est constitué :

1. Du présent référentiel basé sur :
    - La délibération n° 2020-139 du 3 décembre 2020 pour les critères d'évaluation selon le référentiel CNIL ;
    - Le guide de lecture des critères du référentiel de certification des prestataires de formation à la protection des données à caractère personnel ;
    - La délibération n° 2022-026 du 27 janvier 2022 portant adoption des exigences du référentiel d'agrément des organismes de certification pour la certification des prestataires de formation à la protection des données à caractère personnel.

2. Du règlement de la marque Apave Certification et marques d'usage déposées par la CNIL.

1.3. Responsabilité du demandeur

Le demandeur doit assurer la maîtrise des phases qui peuvent être sous-traitées.

Lorsque cette certification lui est accordée, il devient titulaire. Le maintien de cette certification est subordonné aux résultats des audits de surveillance et renouvellement définis dans le présent référentiel.

Par la signature de la proposition commerciale, le demandeur s'engage à :

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 Apave Certification ;
b. fournir à Apave 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 le personnel et l'accès aux informations pertinentes relatives aux sous-traitants ;

c. prendre les dispositions nécessaires pour permettre la participation de la CNIL et de l'instance nationale d'accréditation à l'évaluation en tant qu'observateur ;
d. informer Apave 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 (certificat) ;
e. autoriser Apave Certification à communiquer à la CNIL : les informations relatives à la délivrance ou au retrait de la certification (Décision de certification, Enregistrements…) en lien avec le présent référentiel.
f. faire des déclarations sur la certification en cohérence avec la portée de la certification ;
g. ne pas utiliser la certification de ses services d'une façon qui puisse nuire à Apave Certification ni faire de déclaration sur la certification de ses produits que Apave Certification puisse considérer comme trompeuse ou non autorisée;
h. en cas de suspension, de retrait ou à l'échéance de la certification, cesser d'utiliser l'ensemble des moyens de communication qui y fait référence et remplir toutes les exigences prévues par le programme de certification (par exemple renvoi des documents de certification) et s'acquitter de toute autre mesure exigée;
i. si le client fournit des copies de documents de certification à autrui, il doit les reproduire dans leur intégralité ou tel que spécifié par le programme de certification;
j. en faisant référence à la certification de ses services dans des supports de communication, tels que documents, brochures ou publicité, se conformer aux exigences de l'organisme de certification et/ou aux spécifications du programme de certification;
k. se conformer à toutes les exigences qui peuvent être prescrites dans le programme de certification du produit relatives à l'utilisation des marques de conformité et aux informations relatives au produit;

l. conserver un enregistrement de toutes les réclamations dont il a eu connaissance concernant la conformité aux exigences de certification et mettre ces enregistrements à la disposition de l'organisme de certification sur demande, et :
    - prendre toute action appropriée en rapport avec ces réclamations et les imperfections constatées dans les services qui ont des conséquences sur leur conformité aux exigences de la certification;
    - documenter les actions entreprises.

m. informer, sans délai, l'organisme de certification des changements qui peuvent avoir des conséquences sur sa capacité à se conformer aux exigences de la certification (par exemple, la propriété ou le statut juridique, commercial, et/ou organisationnel, l'organisation et la gestion, les changements apportés au service, les coordonnées de la personne à contacter et les sites de réalisation, les changements importants apportés au système de management de la qualité).

n. disposer de tous les éléments de preuves permettant d'attester de la conformité au référentiel et susceptibles d'être demandés par l'auditeur lors de l'audit. L'absence de preuve le jour de l'audit fera l'objet d'une non-conformité.

2. Contexte réglementaire et normatif

Textes réglementaires :

- Loi n° 2018-771 du 05/09/2018
- Délibération n° 2020-139 du 3 décembre 2020 de la CNIL
- Référentiel - Certification des prestataires de formation à la protection des données personnelles adoptées par la délibération n° 2020-139 du 3 décembre 2020
- Référentiel - Agrément des organismes pour la certification des prestataires de formation à la protection des données adopté par la délibération n° 2022-026 du 27 janvier 2022
- Guide de lecture des critères du référentiel de certification des prestataires de formation à la protection des données à caractère personnel publié par la CNIL
- Arrêté du 6 juin 2019 relatif aux modalités d'audit associées

Textes applicables à l'organisme de certification :

- Norme NF EN ISO/CEI 17065 – Évaluation de la conformité -- Exigences pour les organismes certifiant les produits, les procédés et les services
- Document Cofrac CERT CPS REF 50 – Exigences spécifiques pour l'accréditation des organismes procédant à la certification des prestataires de formation à la protection des données à caractère personnel

Reconnaissances d'Apave Certification :

Apave Certification est un organisme de certification agréé par la Commission Nationale de l'Informatique et des Libertés (CNIL) sur la base de la norme ISO 17024. Cet agrément est valide depuis le 21 novembre 2019 (N° d'agrément : 2019-138) pour la certification des compétences du DPO. En tant que tel, Apave Certification se soumet au contrôle qualité de la CNIL et s'engage à respecter les référentiels qu'elle a défini.

Apave Certification est accrédité par le COFRAC (Comité français d'accréditation) selon les normes :

- ISO 17024 pour la Certification des personnes et compétences, accréditation n°4-0521, portée disponible sur www.cofrac.fr.

- ISO 17021 pour la Certification des systèmes de management accréditations n°4-0552, portée disponible sur www.cofrac.fr.

- ISO 17065 pour les activités de certification de produits et services accréditation 5-0587 portée disponible sur le site www.cofrac.fr.

Apave Certification est reconnu par l'IECEE (IEC System of Conformity Assesment Schemes for Electrotechnical Equipment and Components) dans le schéma CB de certification des produits électriques.

Apave Certification s'engage formellement à prévenir tout conflit d'intérêt selon les dispositions propres aux Organismes Certificateurs.

3. Historique du référentiel

Le présent référentiel porte la référence AC-REF-014-xx, ces derniers chiffres indiquant l'indice de version.

Le tableau ci-dessous indique les principales évolutions apportées pour chaque version du référentiel.

Version	Modifications apportées au référentiel
01	Création
01 Ed. 1	Corrections diverses dans le cadre de la norme d'accréditation COFRAC
01 Ed. 2	Modification des durées d'audit
01 Ed. 3	Suppression de l'EN 9100 et sa portée d'accréditation. Harmonisation des reconnaissances.

4. Candidature de l’organisme

Le candidat à la certification transmet à Apave Certification les informations nécessaires à l’établissement d’une offre commerciale via la « carte d’identité d’organisme », formulaire Apave Certification AC-IMP-294.

Apave Certification transmet au candidat sa proposition commerciale. Si le candidat l’accepte, Apave certification propose, dans les 30 jours, une planification de l’audit en accord avec la date d’audit souhaitée par le candidat.

5. Exigences de certification

Ce chapitre constitue la liste des critères auxquels un prestataire de formation devra démontrer sa conformité en vue d'obtenir la certification de prestataire de formation à la protection des données à caractère personnel selon le référentiel de la CNIL.

1. Exigences générales

C01	Le prestataire est en conformité avec les critères du référentiel national qualité mentionné à l'article L. 6316-3 du code du travail pour ses actions de formation concourant au développement des compétences. Lorsque le prestataire ne dispose pas d'une certification, selon le référentiel national qualité, en cours de validité pour ses actions de formation concourant au développement des compétences, le prestataire est en mesure de démontrer que chaque exigence de celui-ci est respectée pour les formations à la protection des données qu'il propose.
C02	Lorsque le prestataire fait appel à la sous-traitance ou au portage salarial, il s'assure du respect des critères du présent référentiel par le sous-traitant ou le salarié porté, préalablement à la première prestation et ensuite, à des fréquences régulières établies par le prestataire. Note : cela n'implique pas une obligation de certification des sous-traitants.
C03	Le prestataire définit, met en œuvre et maintient à jour des procédures permettant de démontrer le respect des règles relatives à la protection des données pour les traitements qu'il met en œuvre dans le cadre de son activité de formation à la protection des données à caractère personnel. Est notamment couverte par ces procédures la mise en œuvre des mesures de protection des données dans le cadre des traitements de données réalisés pour : - l'évaluation des compétences des intervenants et des apprenants ; - les actions de communication du prestataire à destination du public.

2. Exigences relatives à l'information du public sur les formations proposées

C04	Le prestataire conçoit et propose au moins une formation à la protection des données qui couvre la totalité des objectifs du référentiel général d'aptitudes et de compétences figurant en annexe 1.
C05	Lorsque le prestataire propose une formation qui ne couvre pas à la totalité des objectifs du référentiel général d'aptitudes et de compétences figurant en annexe 1, il informe les apprenants et leur commanditaire de ces exclusions et des pré requis qui en découlent.

3. Exigences relatives à l'identification des besoins et des objectifs de formation

C06	Le prestataire définit les objectifs de chaque formation en termes d'acquis d'aptitudes et de compétences. Le cas échéant, ces acquis d'aptitudes et de compétences précisent ou complètent le référentiel en annexe 1.
C07	Le prestataire définit et met en place une procédure permettant de recueillir et d'analyser les besoins de formation, en matière de protection de données, des apprenants et de leur commanditaire, en vue d'identifier des objectifs de formation. Lorsqu'une demande de formation porte sur une prestation préexistante, le prestataire : - s'assure que les objectifs de cette formation sont adaptés au besoin des apprenants et du commanditaire ; - recueille leurs besoins spécifiques en fonction desquels il peut proposer d'intégrer à la formation des objectifs complémentaires.

	Note : cela n'implique pas l'obligation de concevoir ou d'adapter une prestation préexistante à tous les objectifs identifiés à l'occasion du recueil du besoin. En revanche, si la prestation n'est pas totalement adaptée aux besoins exprimés par les apprenants et leur commanditaire, ceux-ci doivent être informés des objectifs qui ne seront pas couverts par la formation proposée.
C08	Lorsque les objectifs d'une formation visent spécifiquement un secteur d'activité, une thématique particulière ou un type particulier d'opération de traitement de données, le prestataire identifie les compétences spécifiques nécessaires à la conception, à l'adaptation et à la réalisation de cette formation. Note : la liste informative des secteurs d'activité, des thématiques particulières et des types particuliers d'opération de traitement de données publiée par la CNIL peut être utilisée à cette fin.
C09	Le prestataire qui décide de concevoir une formation préparant à une certification de compétences approuvée par la CNIL prend en compte les critères de cette certification lors de la définition des objectifs de la formation.

4. Exigences relatives à la conception des formations

C10	Le prestataire établit le contenu des formations et les méthodes mobilisées, qui incluent une dimension théorique et pratique, en tenant compte des objectifs convenus avec les apprenants et leur commanditaire lors de la phase d'analyse des besoins. Lorsque le prestataire conçoit une formation dont les objectifs portent sur un secteur spécifique, une thématique particulière ou un type particulier d'opération de traitement de données, il prend en compte les référentiels applicables publiés par la CNIL et le Comité européen de la protection des données.
C11	Le prestataire élabore et documente les modalités d'évaluation de l'atteinte par les apprenants des objectifs de chaque formation. En particulier, le prestataire s'assure que les modalités d'évaluation couvrent la totalité des objectifs de chaque formation.
C12	Le prestataire réalise une veille de l'actualité en matière de protection des données, de la législation applicable à la protection des données et de l'état de l'art en matière de sécurité de l'information. Le prestataire identifie régulièrement les formations impactées par les nouveautés identifiées.
C13	Le prestataire revoit et met à jour le contenu des formations en fonction : - de l'évolution des besoins et des retours des apprenants et de leur commanditaire ; - du résultat des évaluations des apprenants ; - de l'actualité en matière de protection des données : lignes directrices du Comité européen de la protection des données, référentiels élaborés par la CNIL, communications et mesures correctives de la CNIL, etc. ; - de l'évolution de la législation en matière de protection des données ; - du développement des techniques en matière de sécurité de l'information ; - de l'évolution des menaces en matière de sécurité de l'information.
C14	Le prestataire s'assure que le contenu des formations a été actualisé depuis moins de 3 mois au moment de leur réalisation.
C15	Lors de la modification ou de l'adaptation des objectifs d'une formation, le prestataire s'assure que le contenu de cette formation et les modalités d'évaluation restent adéquats.
C16	Le prestataire mobilise des concepteurs qui disposent des compétences nécessaires à l'atteinte des objectifs identifiés, notamment s'agissant des secteurs spécifiques et des thématiques particulières ou types particuliers d'opérations de traitement.
C17	Le prestataire s'assure que les évolutions du contenu de chaque formation et des modalités d'évaluation font l'objet d'un suivi qui permet la maîtrise des modifications, par exemple par contrôle des versions. Le prestataire documente l'objet des modifications apportées, la date d'application de ses modifications et leurs auteurs.

5. Exigences relatives à la préparation et à l'adaptation des formations aux apprenants

C18	Lorsque la demande de formation porte sur une prestation préexistante, le prestataire adapte le contenu de la formation aux objectifs complémentaires convenus avec les apprenants et leur commanditaire lors de la phase d'analyse des besoins.
C19	Le prestataire mobilise des formateurs qui disposent des compétences nécessaires à l'atteinte des objectifs identifiés, notamment s'agissant des secteurs spécifiques et des thématiques particulières/types particuliers d'opérations de traitement, et en prenant en compte les besoins des apprenants. Lorsque le prestataire souhaite faire appel à des intervenants qui ne remplissent pas les critères de compétences des formateurs du présent référentiel (intervenant « hors critères »), ou que l'organisme n'est pas en mesure de démontrer le respect de ces critères pour ces intervenants, il s'assure que les interventions concernées font l'objet d'une évaluation par un formateur répondant aux critères de compétences du présent référentiel (formateur « qualifié »). Cette évaluation vise à analyser la pertinence de l'intervention pour l'atteinte des objectifs de la formation, en complément des interventions réalisées par les formateurs mobilisés pour la prestation. Pour les interventions régulières, cette évaluation est renouvelée tous les ans. Note : tout recours à des intervenants « hors critères » doit être justifié par une intervention nécessitant un profil d'intervenant spécifique.

6. Exigences relatives aux conditions de réalisation des formations

C20	Le prestataire tient une liste des sessions de formations à la protection des données qui ont été réalisées. Cette liste inclut notamment la date, la référence de la formation, le nom des intervenants et le nombre d'apprenants ayant terminé la formation.

7. Exigences relatives aux compétences des intervenants

C21	Le prestataire s'assure que son personnel possède les compétences requises pour recueillir les besoins des apprenants et de leur commanditaire, définir les objectifs des formations demandées et identifier les secteurs spécifiques, les thématiques particulières ou les types particuliers d'opérations de traitement.
C22	Le prestataire s'assure que les concepteurs du contenu des formations, les concepteurs des modalités d'évaluation et les formateurs ont une expérience professionnelle qui inclut : - (profil « technique ») au moins 3 ans dans des postes ou des fonctions dédiées à la conception, ou à l'évaluation ou à la mise en œuvre de mesures relatives à la sécurité de l'information ; ou - (profil « juridique ») au moins 3 ans dans des postes ou des fonctions dédiées à l'analyse, ou à l'évaluation ou à la mise en œuvre de la réglementation applicable à la protection des données à caractère personnel. Lorsqu'une formation est conçue ou réalisée par un unique intervenant, le prestataire s'assure que cet intervenant dispose d'une expérience professionnelle qui permet de justifier d'une expérience correspondant à la fois aux profils « technique » et « juridique » définis par le présent référentiel. Le prestataire s'assure que cette expérience professionnelle n'est pas antérieure à 2 ans au moment de l'intervention. Note : les expériences professionnelles acquises en tant que stagiaire ou apprentis ne sont pas comptabilisées.

C23	Le prestataire s'assure que les concepteurs et les formateurs justifient : - a minima d'un diplôme en droit de niveau Master 2 ou équivalent ; ou - a minima d'un diplôme de niveau Master 2 ou équivalent dans le domaine de l'informatique, des systèmes d'information ou de la cybersécurité ; ou - d'une formation diplômante relative à la protection des données à caractère personnel. À défaut de justifier d'un de ces diplômes, les concepteurs et les formateurs doivent justifier au titre de la validation des acquis de l'expérience dans le contexte de ce référentiel : - d'une expérience professionnelle à plein temps d'au moins 5 ans dans des postes ou des fonctions dédiées à la conception, ou à l'évaluation ou à la mise en œuvre de mesures relative à la sécurité de l'information ; ou - d'une expérience professionnelle à plein temps d'au moins 5 ans dans des postes ou des fonctions dédiées à l'analyse, ou à l'évaluation, ou à la mise en œuvre de la réglementation applicable à la protection des données à caractère personnel. Note : S'agissant des compétences des concepteurs et des formateurs, les critères d'expérience professionnelle (C22), de formation ou de validation d'acquis d'expérience (C23), d'expérience pédagogique (C24) et d'entretien des connaissances (C25) sont cumulatifs : le prestataire doit être en capacité de démontrer que ces critères sont individuellement respectés pour chacun de ces intervenants.
C24	Le prestataire s'assure que les concepteurs et les formateurs : - ont conçu ou animé une formation diplômante ; ou - ont conçu ou animé une formation réalisée par un prestataire certifié selon le présent référentiel (ou labelisée par la CNIL) ; ou - font l'objet d'une évaluation de leurs aptitudes pédagogiques à l'occasion de leur première intervention dans le cadre d'une formation à la protection des données.
C25	Le prestataire s'assure que les concepteurs et formateurs entretiennent leurs connaissances en matière de protection des données.
C26	Le prestataire fixe les critères permettant d'identifier les compétences des concepteurs et formateurs en matière de protection des données à caractère personnel dans les secteurs spécifiques, pour les thématiques particulières ou les types particuliers d'opérations de traitement pour lesquels il souhaite répondre aux besoins de formation.

8. Exigences relatives au recueil des appréciations et la prise en compte des réclamations

C27	Le prestataire définit et met en place une procédure pour recueillir et traiter le retour des apprenants, sur les ressources mobilisées (documentaires et humaines) ainsi que sur la capacité de la formation à répondre à leurs besoins et aux objectifs identifiés.
C28	Le prestataire définit et met en place une procédure destinée à recueillir et traiter les réclamations concernant l'activité de formation à la protection des données à caractère personnel. Le prestataire accuse réception des réclamations. Il répond aux demandeurs et tient les plaignants informés de la conclusion du traitement de leur réclamation dans un délai maximum de 2 mois à compter de la date de réception de leur envoi et les informe, au cours de cette période, de l'évolution du traitement de leur demande ou de leur réclamation. Lorsque le traitement de la réclamation est complexe, ce délai peut être prolongé. Dans ce cas, le prestataire informe le plaignant du délai supplémentaire au terme duquel une réponse lui sera transmise et des motifs qui justifient ce délai supplémentaire. Il informe le plaignant de cette prolongation dans le mois suivant réception de la réclamation.
C29	Le prestataire désigne une personne chargée de faire office de point de contact pour la CNIL sur les questions relatives à la certification.

Annexe 1 : Référentiel général d'aptitudes et de compétences

1. La protection des données, ses notions clés et ses acteurs

AC01	La formation permet de connaître et de comprendre les notions de : Données à caractère personnel ; Catégories particulières de données à caractère personnel ; Données relatives aux condamnations pénales et aux infractions ; Traitement de données à caractère personnel ; Fichier ; Responsable de traitement ; Sous-traitant ; Destinataire ; Tiers autorisé ; Droits des personnes ; Profilage ; Anonymisation ; Pseudonymisation ; Authentification ; Habilitation ; Journalisation ; Archivage ; Chiffrement.
AC02	La formation permet d'identifier les traitements de données à caractère personnel.
AC03	La formation permet de connaître et de comprendre les principes permettant qualifier les parties prenantes à un traitement (responsables de traitement, les responsables conjoints, les sous-traitants, destinataires).
AC04	La formation permet de connaître et de comprendre les différentes missions des autorités de contrôle et du Comité européen de la protection des données.
AC05	La formation permet de connaître et de comprendre le champ d'application matériel et territorial du règlement européen de la protection des données.
AC06	La formation permet de connaître et de comprendre l'articulation entre les textes relatifs à la protection des données et les autres sources de droit.
AC07	La formation permet de connaître et de comprendre les principes applicables aux transferts de données hors de l'Union européenne et de l'Espace économique européen (EEE).
AC08	La formation permet d'identifier l'existence de transferts hors de l'Union européenne et de connaître les différents instruments juridiques permettant de les encadrer.

2. Les principes de la protection des données

AC09	La formation permet de connaître et de comprendre les conditions de licéité d'un traitement.
AC10	La formation permet de connaître et de comprendre les conditions applicables au consentement.
AC11	La formation permet de connaître et de comprendre le principe finalité et d'identifier un détournement de finalités.
AC12	La formation permet de connaître et de comprendre le principe de proportionnalité et de pertinence des données.
AC13	La formation permet de connaître et de comprendre les conditions applicables aux traitements portant sur des catégories particulières de données.
AC14	La formation permet de connaître et de comprendre le principe de durée de conservation des données.
AC15	La formation permet de connaître et de comprendre les principes de sécurité et de confidentialité des données et permet de qualifier un incident de sécurité en violation de données à caractère personnel.
AC16	La formation permet de connaître et de comprendre le principe de transparence des informations et des communications avec les personnes concernées par un traitement.
AC17	La formation permet de connaître et de comprendre les droits dont disposent les personnes concernées ainsi que leurs modalités d'exercice : le droit d'accès ; le droit de rectification ; le droit à l'effacement ; le droit à la limitation du traitement ; le droit à la portabilité ; le droit d'opposition.

AC18	La formation permet de connaître et de comprendre le principe d'exactitude des données.

3. Les responsabilités des acteurs

AC19	La formation permet de connaître et de comprendre le principe de responsabilité (« accountability »/redevabilité) et les mesures organisationnelles, règles internes et outils de la conformité permettant de s'assurer et de démontrer que les règles relatives à la protection des données sont respectées.
AC20	La formation permet d'identifier des mesures de protection des données dès la conception et par défaut.
AC21	La formation permet de connaître et de comprendre les obligations incombant aux responsables de traitement et le principe de responsabilité conjointe.
AC22	La formation permet de connaître et de comprendre les obligations incombant aux sous-traitants.

4. Le DPO et les outils de la conformité

AC23	La formation permet de connaître et de comprendre la méthodologie de l'analyse d'impact relative à la protection des données.
AC24	La formation permet de connaître et de comprendre les fonctions et missions du délégué à la protection des données.
AC25	La formation permet de comprendre le contenu du registre d'activités de traitement (responsable de traitement), du registre des catégories d'activités de traitement (sous-traitant) et du registre des violations de données.
AC26	La formation permet de connaître et de comprendre les garanties apportées par les codes de conduite et les mécanismes de certification lorsqu'ils sont approuvés par une autorité ou par le Comité européen de la protection des données.

5. Sources de veille

AC27	La formation permet de connaître les moyens permettant de s'informer sur l'actualité et la jurisprudence en matière de protection des données.
AC28	La formation permet de connaître les moyens permettant de s'informer sur l'état de l'art en matière de sécurité de l'information.

6. Evaluation tierce partie par Apave Certification

La certification « La certification des prestataires de formation à la protection des données à caractère personnel», est attribuée par Apave Certification aux prestataires évalués conformes aux dispositions du présent référentiel.

La certification des prestataires de formation peut être associée à la certification Qualiopi dans le cadre d'un audit initial conjoint ou dissocié pour les deux référentiels ou pour la certification d'un organisme déjà certifié Qualiopi (voir § 6.4) et peut être réalisée sur site ou à distance selon la procédure AC-MOP-027-Guide audit à distance.

Chaque certification fait l'objet d'un dossier spécifique au sein d'Apave Certification (rapport d'audit, certificat).

Le certificat est délivré pour 3 ans suite à l'audit initial et est maintenu sous réserve de la réalisation des audits de suivi et renouvellement.

Lorsque l'évaluation est réalisée en complément d'une certification préexistante selon le référentiel Qualiopi (ou simultanément), Apave 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 Qualiopi, telles que définies dans le présent référentiel, soient respectées.
Apave Certification s'assurera de la conformité du prestataire de formation aux critères de certification approuvés par la CNIL. En particulier :

- avoir accès à la totalité de la grille d'audit selon le référentiel Qualiopi (et pas uniquement au certificat de conformité ou à une attestation similaire) ;
- documenter ses propres constats en faisant référence aux résultats pertinents de la grille d'audit préexistante;
- 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 Qualiopi sont identifiés, l'évaluation est étendue aux critères de certification concernés.
Le cas échéant Apave Certification documentera ses constats dans un rapport d'évaluation qui comprend :

- la liste des formations à la protection des données proposées et/ou réalisées ;
- le plan d'évaluation (incluant les mises à jour réalisées pendant l'évaluation) ;
- les références aux documents et enregistrements examinés ;
- les formations échantillonnées ;
- la fonction des personnes ayant fait l'objet d'un entretien ;
- 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.

Apave Certification sollicitera 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 au moment de sa décision de certification.
Le plan d'action résultant de la décision de certification est également annexé au rapport d'évaluation. Ce plan d'action est examiné par Apave Certification avant la revue et la décision de certification.

6.1. Audit initial

L'audit est réalisé dans les locaux du prestataire de formation ou à distance. 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 Qualiopi (ou lorsque qu'elle est réalisée simultanément en vue d'obtenir la certification Qualiopi), l'évaluation des critères de certification approuvés par la CNIL peut être réalisé à distance, sous réserve que les conditions de prise en compte de la certification Qualiopi soient respectées.

Audit du respect des exigences du référentiel selon une check-list (définie à partir des éléments listés en § 5) permettant d'établir la conformité du dispositif au référentiel et de délivrer le certificat.

Audit du siège et des lieux de mise en œuvre des activités, examen et évaluations des dispositions organisationnelles et des pratiques relatives aux thématiques figurant dans le référentiel de certification :

Description	**Délai**
● Planification, préparation de l'audit	Proposée dans les 30 jours après la signature du contrat initial
● Réalisation de l'Audit	
● Rédaction du rapport	Dans les 15 jours suivant l'audit
● Réponse de l'organisme aux non-conformités éventuelles	Dans les 15 jours suivant la réception du rapport
● Vérification des plans d'actions par l'auditeur	Dans les 15 jours suivant la réception des réponses de l'organisme
● Décision de certification	Environ 60 jours suivant l'audit

Durée de l'audit : Voir § 6.4

6.2. Audit de suivi

L'audit de surveillance est réalisé entre le 14e et le 22e mois suivant la date d'obtention de la certification.

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

- signalements ou de réclamations,
- résultats d'une analyse de risque issue de l'audit précédent.

NB : L'analyse de risque réalisée dans le cadre d'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.

L'audit de surveillance permet de vérifier, une fois la certification délivrée, que le référentiel en vigueur est toujours appliqué. Une attention particulière est prêtée aux non-conformités identifiées lors du précédent audit ainsi qu'à l'efficacité des actions correctives et des mesures préventives du plan d'action mises en place.

L'auditeur conduit l'analyse:

- des éléments administratifs relatifs à l'activité de l'organisme;
- de la conformité au référentiel par l'analyse d'une ou plusieurs actions conduites depuis le précédent audit;
- des actions conduites dans le cadre de la démarche d'amélioration de l'organisme.

Description	**Délai**
● Planification, préparation de l'audit	
● Audit	Entre le 14ème et 22ème mois après la date décision de certification
● Rédaction du rapport	Dans les 15 jours suivant l'audit
● Réponse de l'organisme aux non-conformités éventuelles	Dans les 15 jours suivant la réception du rapport
● Vérification des plans d'actions par l'auditeur	Dans les 15 jours suivant la réception des réponses de l'organisme
● Décision de certification	Environ 60 jours suivant l'audit

Durée de l'audit : Voir § 6.4

6.3. Audit de renouvellement

Avant l'échéance du certificat de 3 ans, un audit de renouvellement est réalisé selon les mêmes règles que l'audit initial.

Description	**Délai**
● Planification, préparation de l'audit	Proposée dans les 30 jours après la signature du contrat de renouvellement, idéalement 2 mois avant l'échéance du certificat
● Audit sur site	
● Rédaction du rapport	Dans les 15 jours suivant l'audit sur site
● Réponse de l'organisme aux non-conformités éventuelles	Dans les 15 jours suivant la réception du rapport
● Vérification des plans d'actions par l'auditeur	Dans les 15 jours suivant la réception des réponses de l'organisme
● Décision de certification	Environ 60 jours suivant l'audit sur site

Durée de l'audit : Voir § 6.4

6.4. Durée des audits

Le tableau ci-dessous se rajoute aux 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 Qualiopi 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 Qualiopi précitées (initial ou renouvellement), s'ajoute à minima 1 jour d'évaluation pour :

- les prestataires de formation non certifiés selon le référentiel Qualiopi ;
- les prestataires certifiés selon le référentiel Qualiopi 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 Qualiopi précitées (surveillance), s'ajoute à minima 0,5 jour d'évaluation selon les mêmes conditions (à savoir pour les prestataires de formation non-certifiés Qualiopi et pour les prestataires certifiés avec plus de 3 formations).

	DUREES D'AUDIT OF RGPD (Ne comprennent pas la durée d'audit Qualiopi)					
	Tranche de CA N-1	Durée d'audit Initial/Renouvellement		Durée d'audit de surveillance		Durée par site secondaire échantillonné
		Nombre de formations "protection des données" au catalogue				
		< = 3	> 3	< = 3	> 3	
Audit associé Qualiopi (Organisme certifié Qualiopi) Audit conjoint ou dissocié	< 150 000 €	1	2	0,5	1	0,5
	150.000 à 750.000 €	1,5	2,5	0,5	1	
	> 750.000 €	2	3	1,5	2	
Audit OF RGPD seul (non certifié Qualiopi)	< 150 000 €	2	2	1	1	
	150.000 à 750.000 €	2,5	2,5	1	1	
	> 750.000 €	3	3	2	2	

Les durées sont exprimées en jours d'audit, d'une durée de 8h.
CA : Chiffre d'affaire annuel relatif à l'activité de prestataire d'action concourant au développement des compétences spécifique au RGPD.
Nombre de formations : formations spécifiques « protection des données personnelles » au catalogue de l'organisme.
Site échantillonné : Durée d'audit pour chaque site échantillonné pour les organisations multisites selon les modalités décrites au § 6.5.
Critères de réduction de durées d'audits :

- un rapport d'un audit selon le référentiel Qualiopi ne présentant aucune non-conformité ;
- une optimisation d'organisation des audits rendue possible par un audit conjoint avec l'évaluation du référentiel Qualiopi ;
- au moins une des formations RGPD est inscrite au Répertoire Spécifique ou au Répertoire National des Certifications Professionnelles de France Compétences.

6.5. Organismes multisites

Un organisme multisites est couvert par un seul système qualité comprenant une fonction centrale (pas nécessairement le siège) qui régit plusieurs sites sur lesquels tout ou partie des activités (administrative, commerciale ou ingénierie) entrant dans le champ de la certification sont réalisées. Un site est caractérisé par la présence permanente de personnel de l'organisme.

Un organisme multisites n'est pas nécessairement une seule entité juridique, mais tous les sites concernés ont un lien juridique ou contractuel avec la fonction centrale de l'organisme. Ils font l'objet d'une surveillance régulière définie par la fonction centrale qui est responsable des mesures correctives nécessaires sur les sites. La fonction centrale doit veiller à ce que les données de chaque site soient collectées et analysées, et doit être capable de démontrer son autorité et sa capacité à amorcer au besoin des changements organisationnels.

Pour être qualifié de multisites:

- l'organisme candidat doit avoir un seul et unique système qualité;
- l'organisme candidat doit identifier sa fonction centrale qui fait partie de l'entité et n'est pas sous-traitée;
- la fonction centrale doit avoir l'autorité organisationnelle pour définir, mettre en place et faire fonctionner le système qualité unique;
- tous les sites doivent être inclus dans le programme de surveillance géré par la fonction centrale.

L'échantillonnage d'un panel de sites est autorisé si les conditions d'éligibilité mentionnées ci-dessus sont démontrées. L'échantillonnage d'un panel de sites est représentatif de la variété des sites. L'échantillonnage est constitué, hors la fonction centrale auditée lors de chaque audit du cycle, selon les modalités suivantes:

- audit initial et de renouvellement: l'échantillon est la racine carrée du nombre total de sites et arrondi à l'entier le plus proche, choisis aléatoirement par Apave Certification;
- audit de surveillance: l'échantillon est la racine carrée du nombre total de sites multiplié par 0,6 et arrondi à l'entier le plus proche, choisis aléatoirement par Apave Certification. L'audit comprend à minima un site non audité à l'audit précédent.

Dans tous les cas, Apave Certification peut décider d'auditer un site particulier s'il le juge pertinent.

Si une non-conformité est identifiée sur un site, la fonction centrale doit déterminer si les autres sites peuvent être affectés par cette non-conformité. Si c'est le cas, des mesures correctives sont mises en oeuvre sur les sites concernés et vérifiées par la fonction centrale. Si ce n'est pas le cas, la fonction centrale démontre à l'organisme certificateur pourquoi elle limite son suivi des actions correctives.

Au moment du processus de prise de décision, si un ou plusieurs sites présente(nt) une non- conformité majeure, la certification est refusée à l'ensemble de l'organisme multisites jusqu'à ce que celui-ci prenne des mesures correctives satisfaisantes.

Il est interdit d'exclure un site du périmètre de la certification.

Si un nouveau site demande à rejoindre un organisme multisites certifié, ce site doit être audité avant d'être inclus dans le certificat, en plus de la surveillance prévue dans le plan d'audit. Après intégration du nouveau site sur le certificat, il doit être ajouté aux sites du périmètre pour déterminer la taille de l'échantillon et la durée des prochains audits de surveillance ou de renouvellement.

6.6. Non conformités

Une non-conformité est un écart par rapport à un ou plusieurs indicateurs du référentiel. Elle peut être mineure ou majeure.

- Une non-conformité **mineure** est la prise en compte partielle d'un indicateur ne remettant pas en cause la qualité de la prestation délivrée.
- Une non-conformité **majeure** est la non prise en compte d'un indicateur ou sa prise en compte partielle remettant en cause la qualité de la prestation délivrée.

Une certification peut être suspendue ou retirée, au regard de la gravité et/ou du nombre ou de la récurrence de non-conformités détectées, dans le cas de non conformités majeures non levées sous trois mois ou de non conformités mineures déjà détectées pour lesquelles l'organisme n'a pas proposé ou mis en œuvre des actions correctives efficaces.

Les délais de mise en œuvre des actions correctives ne doivent pas dépasser un délai fixé en fonction du niveau de gravité des non-conformités:

- pour une non-conformité mineure : le plan d'action établi est adressé à l'organisme certificateur dans le délai fixé par ce dernier et doit être mis en œuvre dans un délai de six mois. La vérification de la mise en œuvre des actions correctives est faite 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 d'actions correctives doit être effective sous trois mois. A défaut de mise en œuvre des actions correctives, la certification est non attribuée ou suspendue. La suspension de la certification est levée par l'organisme certificateur suite à la réception de preuves permettant de constater le retour en conformité par le prestataire et le solde des non conformités majeures. A défaut de mise en œuvre des actions correctives dans un délai de trois mois après la suspension, la certification est retirée ou elle n'est pas délivrée. Elle nécessite alors la réalisation d'un nouvel audit initial de certification.

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

L'existence d'au moins cinq non-conformités mineures non levées à la prise de décision constitue une non-conformité majeure. Une certification ne peut être délivrée tant qu'il reste une non-conformité majeure non levée.

6.7. Cas spécifiques

Réduction de périmètre, suspension ou retrait de la certification

En cas de problèmes liés aux conditions de maintien de la certification (écart(s) constaté(s) par rapport aux critères requis et définis dans le référentiel, manquements à la déontologie, utilisation abusive de la marque Apave Certification, refus d'audit complémentaire, transmission hors délais ou pas de réponse aux écarts relevés), de réclamations et/ou de plaintes adressées à la Direction d'Apave Certification, celle-ci peut décider la réduction du périmètre de certification, la suspension ou le retrait du (des) certificat(s) après consultation de l'Expert décisionnaire.

Les décisions de réduction de périmètre, de suspension ou de retrait de certificat sont notifiées par écrit à l'organisme en lui précisant, s'il y a lieu, les conditions et délais dans lesquels il peut à nouveau postuler ou reprendre le processus de certification dans sa totalité ou partiellement.

La suspension, à la demande d'Apave Certification, est décidée pour une durée n'excédant pas 6 mois. Au-delà, elle se transforme en réduction de périmètre de la certification ou en retrait. Elle peut être levée avant le délai et à la demande de l'organisme, dès que celui-ci a justifié que son motif est devenu sans objet.

Dès notification de la sanction, l'organisme n'apparaît plus sur la liste des certifiés (provisoirement ou définitivement) ou son périmètre est modifié.

Un courrier est adressé à l'organisme lui indiquant les motifs de la décision et demandant le retour du(des) certificat(s) original (aux), de ne plus élaborer ou créer de documents techniques ou commerciaux sur lesquels il est fait référence à la certification, de faire disparaître toute mention à la certification sur les documents et supports commerciaux, de ne plus communiquer sur la certification de quelque manière que ce soit et ce quel que soit le support (application de l'article 8 des conditions générales de certification).

En cas de constatation de non exécution des consignes ci-dessus, une lettre de mise en demeure est adressée à l'organisme en recommandée avec AR avant saisie des instances compétentes.
Le site Internet de l'organisme est contrôlé 1 mois après la notification de la sanction.

6.7.1. Transfert

Le transfert d'une certification est la reprise d'une certification existante et valide, par un autre organisme certificateur accrédité ou en cours d'accréditation. L'organisme candidat transmet sa demande au nouvel organisme certificateur souhaité en lui adressant les éléments suivants :

- 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 ;
- la liste des sous-traitants impliqués dans les prestations de formation à la protection des données ;
- les informations relatives à la réalisation des prestations de formation, incluant l'adresse des lieux permanents de gestion, conception et réalisation des formations ;
- une copie du certificat émis ;
- le dernier rapport d'audit ;
- les plaintes reçues

Apave Certification vérifie que les activités certifiées entrent dans le cadre de la portée de son accréditation et le dispositif en vigueur. Il effectue une revue des informations obtenues afin de garantir qu'il possède les compétences nécessaires en matière de protection des données, conformément aux exigences 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.

Le cas échéant, au moment de la demande, Apave Certification s'assure de la validité de la certification obtenue et demande à l'ancien organisme certificateur de lui transmettre sous un délai de quinze jours une copie du certificat émis, un dossier détaillant les non-conformités détectées et le plan d'action associé pour y remédier.

Apave Certification examine alors l'état des non-conformités en suspens, les dernières conclusions d'audit, les réclamations reçues et les actions correctives mises en œuvre. Il décide, dans un délai de trente jours, selon les cas:

- de reprendre le dossier en confirmant la certification, et émet un certificat;
- d'organiser, après analyse du dossier, une évaluation adaptée;
- de refuser la reprise de la certification.

Les motifs de refus sont motivés par écrit à l'organisme.

6.7.2. Extension

L'organisme candidat souhaitant certifier de nouveaux sites, en sus des sites déjà certifiées, sollicite l'extension de sa certification auprès d'Apave Certification.

Un audit d'extension de la certification sur les sites ou les formations de la demande est mis en œuvre pour procéder à l'extension de la certification; cet audit est réalisé à tout moment du cycle de certification. En cas de décision positive, le certificat de l'organisme est mis à jour en conséquence. Le plan d'audit (contenu de l'audit, durée…) pour les audits suivants tient compte de l'extension de la certification.

6.7.3. Engagements d'Apave Certification en cas de suspension/retrait /résiliation d'accréditation ou cessation d'activité

La certification des prestataires de formation à la protection des données à caractère personnel selon le référentiel unique de la CNIL est délivrée par un organisme certificateur ayant répondu aux exigences d'accréditation COFRAC et au référentiel d'agrément CNIL.

En cas de suspension de l'accréditation, Apave Certification s'engage à ne plus délivrer de certificats jusqu'à la levée de la suspension par l'instance nationale d'accréditation. Pendant cette période, Apave 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, Apave Certification n'est plus autorisé à délivrer de certificats. Les certificats déjà délivrés restent valides pendant une période de 6 mois. Les prestataires de formation titulaires d'un certificat délivré ou en cours de certification sont informés par Apave Certification. Ceux-ci pourront choisir un autre organisme certificateur accrédité ou en cours d'accréditation par une instance nationale d'accréditation pour lui transférer leur certification.

7. Communication

La communication par l'organisme de formation devra se faire selon le règlement d'usage de la marque Apave Certification (AC-REG-001) et les règles d'usage des marques déposées par la CNIL à destination des prestataires de formation certifiés, en prenant notamment en compte les éléments suivants:

Supports de communication	**Mentions devant figurer sur ces supports**
1. Le certificat Apave Certification : Il doit être affiché à la vue des usagers dans les locaux du certifié. Ce document est élaboré par Apave Certification.	· La marque de certification  . L'adresse d'Apave Certification, 6 Rue du Général Audran CS 60123 - 92412 Courbevoie · Les coordonnées de l'organisme certifié · L'identification précise du référentiel : codification indiquée sur le référentiel en vigueur . Le périmètre précis relatif aux formations à la protection des données à caractère personnel proposées par le prestataire et certifiées par Apave Certification.
2. Documents publicitaires, commerciaux et contractuels, tout support de communication **mentionnant la certification** (exemples : véhicules, cartes de visite, papier à en-tête, factures, site internet…)	· Les coordonnées de l'organisme certifié · La marque de certification  · · Les coordonnées d'Apave Certification : au minimum l'adresse restreinte (92412 Courbevoie) · L'identification précise du référentiel : codification indiquée sur le référentiel en vigueur

8. Transmission de données à la CNIL

Dans le cadre de son accréditation, Apave Certification transmettra les éléments suivant à la CNIL :

- le nom du prestataire de formation et les éléments permettant son identification ;
- la documentation de certification officielle (le certificat émis).

Sur demande de la CNIL, Apave Certification peut être amenée à transmettre à la CNIL des informations supplémentaires en lien avec l'évaluation du client, dans le but de démontrer la conformité du processus de certification aux exigences du présent référentiel.