RÉFÉRENTIEL

DE CERTIFICATION DES « PRESTATAIRES DE FORMATION À LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL »

Décembre 2020

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

À qui s'adresse ce référentiel ?

Ce référentiel 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. Terminologie

Terme	Définition
Apprenant (Bénéficiaire)	Personne engagée dans un processus d'apprentissage (ISO 29993:2017[1]).
Aptitude	Capacité d'appliquer un savoir et d'utiliser un savoir-faire pour réaliser des tâches et résoudre des problèmes (Guide RNQ[2]).
Compétence	Capacité avérée de mettre en œuvre des savoirs, des savoir-faire et des dispositions personnelles, sociales ou méthodologiques dans des situations de travail ou d'études/formations, pour le développement professionnel ou personnel (Guide RNQ).
Objectifs de formation	Enoncé des aptitudes et compétences, visées et évaluables, qui seront acquises au cours de la formation (Guide RNQ).
Commanditaire de la formation	Organisation ou individu qui fait l'acquisition de services de formation pour le compte d'apprenants, qui leur assure un soutien financier ou autre, ou qui a un intérêt direct dans le résultat de l'apprentissage (ISO 29993:2017).
Prestataire de services de formation (Prestataire)	Organisme fournissant des services de formation en dehors du cadre de l'enseignement formel, incluant tous les collaborateurs impliqués dans la fourniture du service de formation (ISO 29993:2017).
Service de formation (Formation/Prestation)	Séquence d'activités conçue pour permettre l'apprentissage (ISO 29993:2017)
Formateur	Personne qui travaille avec les apprenants pour les aider dans leur apprentissage (ISO 29993:2017).
Méthodes mobilisées	Modalités pédagogiques et/ou moyens et/ou outils utilisés pour mener à bien la prestation dispensée (Guide RNQ).
Modalités d'évaluation	Moyens mobilisés pour mesurer à l'aide de critères objectifs les acquis du bénéficiaire en cours et/ou à la fin de la prestation (Guide RNQ).
Concepteur du contenu des formations (Concepteur)	Personne chargée par le prestataire de la conception et de l'adaptation du contenu de la formation et des méthodes mobilisées.
Concepteurs des modalités d'évaluation (Concepteur)	Personne chargée par le prestataire de la conception des modalités d'évaluation.

[1] ISO/IEC 29993 - Services de formation fournis en dehors du cadre de l'enseignement formel -- Exigences de services

[2] « Guide | Référentiel national qualité », travail-emploi.gouv.fr

2. Critères du référentiel

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 prérequis 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.