PROJET DE RÉFÉRENTIEL

DE CERTIFICATION « PRESTATAIRE DE FORMATION A LA PROTECTION DES DONNEES PERSONNELLES »

(Mars 2020)

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

A qui s'adresse ce référentiel ?

Ce projet de référentiel constitue la liste des exigences auxquelles un prestataire de formation devra démontrer sa conformité en vue d'obtenir la certification de prestataire de formation à la protection des données personnelles selon le référentiel de la CNIL.

1. Terminologie

Terme	Définition
Apprenant	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 ou individu 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).
Formateur	Personne qui travaille avec les apprenants (3.8) 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)	Intervenant chargé par le prestataire de la conception et de l'adaptation du contenu de la formation et des méthodes mobilisées.
Examinateur des modalités d'évaluation (Examinateur)	Intervenant chargé par le prestataire d'examiner les modalités d'évaluation en vue d'analyser leur adéquation avec les objectifs d'une formation.

[1] ISO/IEC 29993 - Services de formation fournis en dehors du cadre de l'enseignement formel -- Exigences de services
[2] https://travail-emploi.gouv.fr/demarches-ressources-documentaires/documentation-et-publications-officielles/guides/guide-referentiel-national-qualite

2. Exigences du référentiel

1. Exigences générales	
E01.	Le prestataire dispose d'une certification selon le référentiel national qualité mentionné à l'article L. 6316-3 du Code du travail pour ses actions de formation concourant au développement des compétences.
E02.	Lorsque le prestataire fait appel à la sous-traitance ou au portage salarial, il s'assure du respect de la conformité au présent référentiel par le sous-traitant ou le salarié porté.
E03.	Le prestataire définit, met en œuvre et maintient à jour une procédure interne visant à être en capacité de démontrer à la CNIL le respect des règles relatives à la protection des données pour les traitements qu'il met en œuvre dans le cadre de l'activité de certification. Sont notamment couverts par cette procédure, les traitements des données mis œuvre pour la collecte et le contrôle des compétences des formateurs et des apprenants ainsi que les traitements de données relatifs aux actions de communication de l'organisme de formation à destination du public.
E04.	En particulier, le prestataire met en place des mesures techniques et organisationnelles pour s'assurer du respect du principe de minimisation des données : - lors de la collecte des données auprès des apprenants, puis pour leur conservation ; - dans le cadre des échanges de données avec les formateurs pour l'exercice de leur mission ; - dans le cadre des échanges de données avec les commanditaires.
E05.	Le prestataire fournit des informations aux formateurs, aux apprenants et aux commanditaires qui les renseignent sur les traitements de données réalisés et sur les modalités de l'exercice des droits des personnes concernées. Ces informations sont concises, transparentes, compréhensibles et aisément accessibles à ce public.
2. Exigences relatives à l'information du public sur les formations proposées	
E06.	Le prestataire conçoit et propose au moins une formation à la protection des données qui couvre la totalité des thèmes du référentiel général d'aptitudes et de compétences figurant en Annexe 1. Le prestataire diffuse une information accessible au public concernant cette formation. Cette information précise les prérequis de cette formation, ses objectifs, sa durée, les modalités et délais d'accès, son tarif, les moyens de contacts, les méthodes mobilisées et modalités d'évaluation, la langue dans laquelle cette formation est dispensée ainsi que les conditions d'accessibilité aux personnes handicapées.

E07.	Lorsque le prestataire propose une formation qui ne couvre pas la totalité des thèmes du référentiel général d'aptitudes et de compétences figurant en Annexe 1, il informe les apprenants et leur commanditaire de ces exclusions.
3. Exigences relatives à l'identification des besoins et à l'atteinte des objectifs de formation	
E08.	Le prestataire définit et met en place une procédure permettant de recueillir les besoins de formation, en matière de protection de données, des apprenants et de leur commanditaire, et d'identifier des objectifs de formation. Lorsque la demande porte sur une formation préexistante, le prestataire s'assure que les objectifs de cette formation sont adaptés au besoin des apprenants et de leur commanditaire, recueille les besoins spécifiques et, le cas échéant, identifie les objectifs complémentaires de formation.
E09.	Le prestataire définit les objectifs de chaque formation en termes d'acquis d'aptitudes et de compétences.
E10.	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.
E11.	Le prestataire évalue l'atteinte par les apprenants des objectifs de chaque formation, selon des modalités d'évaluation prédéfinies.
E12.	Le prestataire qui décide de concevoir une formation préparant à une certification de compétences approuvée par la CNIL, prend en compte les exigences de cette certification lors de la définition des objectifs de la formation.
4. Exigences relatives à la conception des formations	
E13.	Le prestataire établit le contenu des formations et les méthodes mobilisées, en tenant compte des objectifs définis et des besoins recueillis auprès des apprenants et de leur commanditaire. 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.
E14.	Le prestataire élabore et documente les modalités d'évaluation de l'atteinte par les apprenants des objectifs de chaque formation. Les modalités d'évaluation font l'objet d'un examen par une personne en charge d'évaluer leur adéquation avec les objectifs de la formation. Cet examinateur n'a pas été impliqué dans la conception de ces formations.
E15.	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.
E16.	Le prestataire revoit et met à jour le contenu de la formation et les méthodes mobilisées 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.
E17.	Le prestataire s'assure que le contenu des formations a été actualisé depuis moins de 3 mois au moment de leur réalisation.
E18.	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.
E19.	Le prestataire mobilise des concepteurs et des examinateurs 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 adaptées aux besoins des apprenants.
E20.	Le prestataire s'assure que le contenu de chaque formation et les modalités d'évaluation sont identifiables, par exemple par contrôle des versions, et permettent la maîtrise des modifications. 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	
E21.	Lorsque la demande de formation porte sur une prestation préexistante, le prestataire adapte le contenu de la formation et les méthodes mobilisées aux besoins complémentaires des apprenants et de leur commanditaire.
E22.	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 exigences de compétences des formateurs du présent référentiel, ou que l'organisme n'est pas en mesure de démontrer le respect de ces exigences pour ces intervenants, il s'assure que les interventions

concernées sont encadrées par un formateur répondant aux exigences de compétences du présent référentiel.

6. Exigences relatives aux conditions de réalisation des formations

E23. Le prestataire s'assure que les formateurs sont informés des méthodes mobilisées à mettre œuvre pour leur intervention et contrôle régulièrement leur application.

E24. Le prestataire tient un registre des sessions de formations à la protection des données: date, référence de la formation, intervenants, nombre d'apprenants ayant terminé la formation.

7. Exigences relatives aux compétences des intervenants

E25. 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.

E26. Le prestataire s'assure que les concepteurs du contenu des formations, les concepteurs des modalités d'évaluation, les examinateurs 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 relative 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 personnelles.

Lorsqu'une formation est conçue, examinée ou réalisée par un unique intervenant, le prestataire s'assure que cet intervenant a une expérience professionnelle qui permet de justifier d'une expérience correspondant à la fois aux profils « technique » et « juridique » définis par le présent référentiel.

E27. Le prestataire s'assure que les concepteurs, examinateurs et 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 personnelles ; ou

- d'une expérience professionnelle à plein temps d'au moins 8 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 8 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 personnelles.

E28. Le prestataire s'assure que les concepteurs, examinateurs et formateurs ont :

- animé ou suivi une formation diplômante en matière de protection des données personnelles depuis moins de 3 ans ; ou
- animé ou suivi une formation réalisée par un prestataire certifié selon le présent référentiel (ou labélisée par la CNIL) depuis moins de 3 ans ; ou
- dispose d'une certification des compétences du délégué à la protection des données en cours de validité.

E29. Le prestataire fixe les critères permettant d'identifier les compétences des concepteurs, examinateurs et formateurs en matière de protection des données personnelles dans les secteurs spécifiques, pour les thématiques particulières ou les types particuliers d'opération de traitement pour lesquels il souhaite répondre aux besoins de formation.

E30. Le prestataire s'assure que les concepteurs, examinateurs et formateurs continuent à se perfectionner professionnellement en matière de protection des données.

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

E31. Le prestataire définit et met en place une procédure pour recueillir et traiter le retour des apprenants sur les méthodes pédagogiques employées, les ressources mobilisées (humaines et techniques), les méthodes mobilisées, ainsi que sur leur efficacité pour atteindre les objectifs de formation et répondre à leurs besoins.

E32. Le prestataire définit et met en place une procédure destinée à recueillir et traiter les demandes et les réclamations concernant l'activité de formation.

Le prestataire accuse réception des demandes et des réclamations. Il répond aux demandeurs et tient dûment informé les plaignants de la conclusion du traitement de leur réclamation dans un délai maximum de trois 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 demande ou de la réclamation est complexe, ce délai peut être prolongé. Dans ce cas, le prestataire informe le demandeur ou le plaignant du délai supplémentaire au terme duquel une réponse lui sera transmise et les raisons qui justifient ce délai supplémentaire. Il informe le demandeur ou le plaignant de cette prolongation avant le terme du délai en cours.

E33. 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

Exigences relatives à la présentation des principes et des définitions
EC01. La formation permet de connaître et de comprendre les notions de : - donnée personnelle ; - traitement de données personnelles ; - limitation du traitement ; - profilage ; - pseudonymisation ; - fichier ; - responsable de traitement ; - sous-traitant ; - destinataire ; - tiers ; - consentement ; - violation de données personnelles ; - données génétiques ; - données biométriques ; - données de santé ; - établissement principal ; - représentant ; - règles d'entreprise contraignantes ; - autorité de contrôle concernée ; - traitement transfrontalier.
EC02. La formation permet de connaître et de comprendre le champ d'application matériel et géographique du règlement européen de la protection des données.
Exigences relatives à la présentation des conditions de licéité des traitements
EC03. La formation permet de connaître et de comprendre le principe de licéité du traitement.
EC04. La formation permet de connaître et de comprendre les principes de loyauté et de transparence.
EC05. La formation permet de connaître et de comprendre le principe de finalité déterminée, explicite et légitime.
EC06. La formation permet de connaître et de comprendre le principe de limitation des finalités.
EC07. La formation permet de connaître et de comprendre le principe de données adéquates et pertinentes
EC08. La formation permet de connaître et de comprendre le principe de minimisation des données.
EC09. La formation permet de connaître et de comprendre le principe d'exactitude des données.
EC10. La formation permet de connaître et de comprendre le principe de limitation de la conservation des données.

EC11.	La formation permet de connaître et de comprendre les principes d'intégrité et de confidentialité.
EC12.	La formation permet de connaître et de comprendre les bases légales possibles d'un traitement
EC13.	La formation permet de connaître et de comprendre la notion de consentement, les modalités de son retrait, les exceptions à son recueil ainsi que les spécificités liées aux enfants.
EC14.	La formation permet de connaître et de comprendre les catégories particulières de données et les conditions dans lesquelles elles peuvent être traitées.
EC15.	La formation permet de connaître et de comprendre les données relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes.
Exigences relatives à la présentation des droits des personnes à l'égard des traitements de données à caractère personnel	
EC16.	La formation permet de connaître et de comprendre le droit à l'information des personnes concernées par un traitement et les obligations qui en résultent pour le responsable de traitement.
EC17.	La formation permet de connaître et de comprendre le droit d'accès dont disposent les personnes concernées par un traitement et les obligations qui en résultent pour le responsable de traitement.
EC18.	La formation permet de connaître et de comprendre le droit de rectification dont disposent les personnes concernées par un traitement et les obligations qui en résultent pour le responsable de traitement.
EC19.	La formation permet de connaître et de comprendre le droit à l'effacement dont disposent les personnes concernées par un traitement et les obligations qui en résultent pour le responsable de traitement.
EC20.	La formation permet de connaître et de comprendre le droit à la limitation du traitement dont disposent les personnes concernées par un traitement et les obligations qui en résultent pour le responsable de traitement.
EC21.	La formation permet de connaître et de comprendre le droit à la portabilité des données dont disposent les personnes concernées par un traitement.
EC22.	La formation permet de connaître et de comprendre le droit d'opposition dont disposent les personnes concernée par un traitement, les modalités de son exercice et les obligations qui en résultent pour le responsable de traitement.