Commission nationale de l'informatique et des libertés

Délibération n° 2011-315 du 6 octobre 2011 portant adoption d'un référentiel pour la délivrance de labels en matière de formation tendant à la protection des personnes à l'égard du traitement des données à caractère personnel

NOR : *CNIA1100013X*

La Commission nationale de l'informatique et des libertés,

Vu la convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, notamment ses articles 11 (3°, *c*) et 13 ;

Vu le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi du 6 janvier 1978, modifiée par la loi n° 2004-801 du 6 août 2004 ;

Vu la délibération n° 2011-249 du 8 septembre 2011 portant modification de l'article 69 du règlement intérieur de la Commission nationale de l'informatique et des libertés et insérant un chapitre IV *bis* intitulé « Procédure de labellisation » ;

Après avoir entendu M. Jean-François Carrez, commissaire, en son rapport, et Mme Elisabeth Rolin, commissaire du Gouvernement, en ses observations,

Formule les observations suivantes :

L'article 11 (3°, *c*) de la loi du 6 janvier 1978 modifiée dispose qu'*« à la demande d'organisations professionnelles ou d'institutions regroupant principalement des responsables de traitements, [...la CNIL] délivre un label à des produits ou à des procédures tendant à la protection des personnes à l'égard du traitement des données à caractère personnel, après qu'elles les a reconnus conformes aux dispositions de la [loi du 6 janvier 1978 modifiée] »*.

La commission a estimé que les demandes faites par des organisations professionnelles ou institutions regroupant principalement des responsables de traitements correspondent à un besoin des professionnels de ce secteur.

C'est la raison pour laquelle la commission accepte de délivrer des labels en matière de formations tendant à la protection des personnes à l'égard du traitement des données à caractère personnel.

L'article 53-3 du règlement intérieur de la commission précise que *« l'examen d'une demande de label est effectué sur la base d'un référentiel établi par la commission. Ce référentiel définit les caractéristiques que doit présenter un produit ou une procédure afin que celui-ci soit reconnu conforme aux dispositions de la loi du 6 janvier 1978 modifiée. Il précise les modalités d'appréciation de cette conformité et, le cas échéant, les particularités relatives aux vérifications subséquentes à la délivrance du label »*.

Par conséquent, la présente délibération fixe le référentiel d'évaluation des formations tendant à la protection des personnes à l'égard du traitement des données à caractère personnel,

Décide que le référentiel permettant l'évaluation des demandes de labels relatifs à des formations tendant à la protection des personnes à l'égard du traitement des données à caractère personnel figure en annexe de la présente délibération, qui est publiée au *Journal officiel* de la République française.

Pour la présidente :
Le vice-président délégué,
E. DE GIVRY

ANNEXE

RÉFÉRENTIEL AUX FINS DE LABELLISATION DES FORMATIONS

Introduction

Une formation est définie comme un processus destiné à produire et à développer les connaissances, les savoir-faire et les comportements nécessaires à la satisfaction d'exigences (définition issue de la norme ISO 10015 « Management de la qualité-lignes directrices pour la formation »).

Une formation informatique et libertés est donc un processus destiné à produire et à développer des connaissances, des savoir-faire et des comportements nécessaires au respect de la loi informatique et libertés. Il est à noter que ledit processus peut se dérouler sur plusieurs jours et comprendre plusieurs modules indépendants les uns des autres.

Le présent référentiel définit les critères et les moyens permettant à la commission de déterminer si les formations faisant l'objet d'une demande de label permettent effectivement d'atteindre un tel objectif.

Il comporte deux parties correspondant aux deux phases de l'évaluation effectuées par la commission et qui portera sur :

– l'activité de formation (exigences sur la méthode, notées « EMxx » dans le chapitre Ier) ;
– le contenu de la formation, qui est composé :
  – d'un module principal de connaissances fondamentales que la formation doit comporter *a minima* dans son *curriculum* pour prétendre au label (exigences sur le contenu du module principal, notées « ECxx » dans le chapitre II) ;
  – de modules complémentaires, que la formation peut également comporter dans son *curriculum* (exigences sur le contenu supplémentaire, notées « ESxx » dans le chapitre III).

Les demandeurs doivent démontrer qu'ils satisfont les exigences du référentiel en fournissant des explications et des éléments de preuves. Ceux-ci pourront prendre la forme d'un extrait d'un référentiel interne, d'un descriptif d'une méthode ou d'une procédure, ou de tout autre document. Pour être valable, la démonstration proposée ne doit pas se contenter de reprendre le contenu des exigences pour indiquer que la formation soumise à l'évaluation est conforme à celles-ci, mais doit faire comprendre en quoi la formation évaluée y répond de manière spécifique et détaillée.

Une partie de ce référentiel (chapitre Ier) est une interprétation de la CNIL de la norme NF ISO 29990 (services de formation dans le cadre de l'éducation et de la formation non formelles – exigences de base pour prestataires de services, 2010), seul le texte original et complet de cette norme, telle que diffusée par AFNOR – accessible via le site internet www.afnor.org – a valeur normative.

Terminologie

Apprenant	Personne engagée dans un processus d'apprentissage (ISO 29990).
Connaissance	Acquisition de capacité par le biais de la formation notamment.
Compétence	Connaissances, compréhension, habiletés ou attitude qui sont observables et/ou mesurables, mises en œuvre et maîtrisées dans une situation de travail donnée et dans le cadre du développement professionnel et/ou personnel (ISO 29990).
Commanditaire de la formation	Organisme ou individu apportant un soutien financier ou autre à l'apprenant ou étant manifestement intéressé par le résultat de l'apprentissage (ISO 29990).
Curriculum	Plan d'étude élaboré par le prestataire de services de formation, qui décrit les objectifs à atteindre, le contenu, les résultats de l'apprentissage, les méthodes d'enseignement et d'apprentissage et les processus d'évaluation (ISO 29990).
Formation	Processus destiné à produire et à développer les connaissances, les savoir-faire et les comportements nécessaires à la satisfaction d'exigences (ISO 10015).
Formateur	Personne travaillant avec les apprenants pour les aider dans leur apprentissage (ISO 29990).
Organisme de formation	Organisme de toute taille ou individu fournissant des services de formation.

1. Référentiel d'évaluation de l'activité de formation

1.1. *Exigences relatives au respect de la loi informatique et libertés par l'organisme de formation*

EM01. L'organisme de formation a mis en place une démarche visant à s'assurer de la conformité à la loi informatique et libertés de l'ensemble des traitements qu'il met en œuvre pour l'ensemble de ses activités, dont la formation.

EM02. L'organisme de formation a procédé aux formalités préalables relatives aux traitements mis en œuvre au titre de la gestion de son personnel et de l'ensemble de ses activités, dont la formation.

EM03. L'organisme de formation informe, dans le respect des dispositions de la loi informatique et libertés, les personnes concernées par les traitements qu'il met en œuvre.

EM04. L'organisme de formation met en place une procédure destinée à gérer les demandes et les réclamations des personnes dont il traite les données.

1.2. *Exigences relatives à l'identification des besoins de formation*

EM05. L'organisme de formation dispose d'une procédure pour tenir compte des besoins des apprenants et de leur commanditaire lors de la conception du contenu de la formation et du processus de formation (par exemple : formulaire de recueil de besoin, étude de marché réunion préparatoire à l'organisation de la formation...).

EM06. L'organisme de formation dispose d'une procédure pour s'assurer que les méthodes et supports de formation utilisés sont appropriés pour atteindre les objectifs énoncés (par exemple : consultation de professionnels de la protection des données, enquête de satisfaction...).

EM07. L'organisme de formation dispose d'une procédure pour que le contenu de la formation et le processus de formation tiennent compte des résultats de la formation (par exemple : évaluation des apprenants, analyse des questionnaires de satisfaction).

1.3. *Exigences relatives au processus de conception de la formation*

EM08. L'organisme de formation doit mettre au point et documenter un *curriculum* et les moyens d'évaluation appropriés de la formation.

EM09. L'organisme de formation dispose de méthodes de formation qui répondent aux objectifs et aux exigences du *curriculum* et tiennent compte des besoins des apprenants.

EM10. L'organisme de formation dispose de procédures destinées à revoir et mettre à jour le contenu de la formation tant en fonction des besoins et retours des apprenants et de leur commanditaire, que de l'actualité, de l'évolution de la législation et du développement des techniques.

1.4. *Exigences relatives à la compétence et à l'évaluation des formateurs*

EM11. L'organisme de formation s'assure que son personnel et ses formateurs possèdent les compétences requises pour identifier les besoins des apprenants, concevoir la formation et délivrer son contenu (par exemple : en auditionnant le formateur, en assistant à une session de formation...).

EM12. L'organisme de formation s'assure que les formateurs ont une expérience professionnelle de cinq ans au minimum dans le secteur de la protection des données.

EM13. L'organisme de formation s'assure que les formateurs ont effectué deux formations au minimum dans les deux dernières années.

EM14. L'organisme s'assure que les formateurs disposent des compétences clés requises et que ces compétences sont entretenues.

EM15. L'organisme de formation met en place des dispositifs d'évaluation des compétences de son personnel et des intervenants. Ce processus est documenté.

EM16. L'organisme de formation dispose d'une procédure pour demander un retour aux apprenants sur les méthodes, les ressources employées, ainsi que sur leur efficacité à produire les résultats de la formation convenus.

EM17. L'organisme de formation s'assure que les procédures d'évaluation choisies et mises en œuvre fournissent des informations fiables sur les compétences de son personnel et des intervenants.

1.5. *Exigences relatives aux conditions de réalisation de la formation*

EM18. L'organisme de formation informe l'apprenant et son commanditaire des objectifs de la formation, de son format, des instruments pédagogiques utilisés et, le cas échéant, des critères d'évaluation utilisés pour l'évaluation.

EM19. L'organisme de formation informe l'apprenant et son commanditaire des prérequis comme les qualifications et l'expérience professionnelle nécessaires à l'apprentissage.

EM20. L'organisme de formation s'assure que les ressources de la formation sont disponibles et accessibles aux apprenants.

2. **Référentiel d'évaluation du contenu du module principal de la formation**

2.1. *Exigences relatives à la présentation des principes et des définitions*

EC01. La formation permet de comprendre et de connaître les notions de traitement, de fichier, de données à caractère personnel, de responsable de traitement et de destinataire.

EC02. La formation permet de comprendre et de connaître le champ d'application matériel de la loi.

EC03. La formation permet de comprendre et de connaître le champ d'application géographique de la loi.

2.2. *Exigences relatives à la présentation des conditions de licéité des traitements*

EC04. La formation permet de comprendre et de connaître le principe de finalité des traitements.

EC05. La formation permet de comprendre et connaître le principe de pertinence et d'adéquation des données à la finalité poursuivie.

EC06. La formation permet de comprendre et de connaître le principe de la conservation limitée des données.

EC07. La formation permet de comprendre et de connaître le principe relatif à la sécurité physique et logique des données, y compris dans un contexte de sous-traitance.

EC08. La formation permet de comprendre et de connaître la notion de consentement, sa nécessité dans le contexte de mise en œuvre d'un traitement et les exceptions à son recueil.

EC09. La formation permet de comprendre et de connaître les données dites sensibles et les conditions dans lesquelles elles peuvent être traitées.

2.3. *Exigences relatives à la présentation des droits des personnes à l'égard des traitements de données à caractère personnel*

EC10. La formation permet de comprendre et de connaître le droit à l'information des personnes concernées par un traitement et les obligations qui en résultent pour le responsable de traitement.

EC11. La formation permet de comprendre et de connaître le droit d'opposition des personnes, les modalités de son exercice et les obligations qui en résultent pour le responsable de traitement.

EC12. La formation permet de comprendre et de connaître le droit d'accès dont disposent les personnes concernées par un traitement et les obligations qui en résultent pour le responsable de traitement.

EC13. La formation permet de comprendre et de connaître le droit de rectification et de suppression dont disposent les personnes concernées par un traitement et les obligations qui en résultent pour le responsable de traitement.

3. **Référentiel d'évaluation du contenu des modules complémentaires de la formation**

3.1. *Exigences relatives à la présentation de la CNIL et de ses missions*

ES01. La formation permet de comprendre et de connaître le statut et la composition de la CNIL.

ES02. La formation permet de comprendre et de connaître l'organisation de la commission plénière, restreinte et des services.

ES03. La formation permet de comprendre et connaître les différentes missions de la CNIL.

3.2. *Exigences relatives à la présentation des formalités préalables à la mise en œuvre des traitements*

ES04. La formation permet de comprendre et de connaître les différents régimes de formalités préalables.

ES05. La formation permet de comprendre et de connaître, pour les différents régimes, les modalités selon lesquelles les formalités doivent être accomplies auprès de la CNIL et la manière dont elle les instruit.

3.3. *Exigences relatives à la présentation de l'encadrement des transferts de données hors de l'Union européenne*

ES06. La formation permet de comprendre et de connaître les principes relatifs au transfert de données hors de l'Union européenne.

ES07. La formation permet de comprendre et de connaître les différents moyens destinés à encadrer les transferts de données.

ES08. La formation permet de comprendre et de connaître les formalités préalables applicables à un transfert de données hors de l'Union européenne.

ES09. La formation permet de comprendre et de connaître les obligations du responsable de traitement concernant l'information des personnes concernées par le transfert hors de l'Union européenne de leurs données.

3.4. *Exigences relatives à la présentation du rôle du correspondant à la protection des données à caractère personnel*

ES10. La formation permet de comprendre et de connaître le statut du correspondant et les différents types de désignation.

ES11. La formation permet de comprendre et de connaître les modalités et la procédure de désignation d'un correspondant.

ES12. La formation permet de comprendre et de connaître les conditions dans lesquelles la liste des traitements doit être tenue par le correspondant.

ES13. La formation permet de comprendre et de connaître les conditions dans lesquelles le correspondant traite les réclamations adressées au responsable des traitements.

ES14. La formation permet de comprendre et de connaître les conditions dans lesquelles le correspondant doit établir le bilan annuel de son activité.

ES15. La formation permet de comprendre et de connaître les conditions dans lesquelles le correspondant alerte le responsable de traitement sur les manquements qu'il constate.

ES16. La formation permet de comprendre et de connaître les relations entre la CNIL et le correspondant.

ES17. La formation permet de comprendre et de connaître les conditions et la procédure relative à la fin de mission du correspondant.

3.5. *Exigences relatives à la présentation de l'encadrement des traitements dans le domaine de la santé*

ES18. La formation permet de connaître et de déterminer le régime de formalités préalables applicable selon que le traitement a pour objet la recherche dans le domaine de la santé (chapitre IX) ou l'évaluation ou l'analyse des pratiques ou des activités de soins et de prévention (chapitre X).

ES19. La formation permet de comprendre et de connaître le contenu du dossier à présenter à la CNIL, que le traitement concerné relève du chapitre IX ou X de la loi.

ES20. La formation permet de comprendre et de connaître les conditions dans lesquelles un traitement de données à caractère personnel ayant pour objet la recherche dans le domaine de la santé doit être mis en œuvre pour respecter les dispositions de la loi.

ES21. La formation permet de comprendre et connaître les cas dans lesquels la commission peut, pour les traitements de recherche médicale, adopter des méthodologies de référence.

ES22. La formation permet de comprendre et de connaître les droits des personnes qui participent à une recherche médicale et notamment le droit à l'information avec, dans certains cas, le recueil de leur consentement, et les obligations qui en résultent pour le responsable de traitement.

ES23. La formation permet de comprendre et de connaître, pour les traitements de recherche médicale, les cas dans lesquels il peut être dérogé à l'obligation d'information prévue par la loi.

ES24. La formation permet de comprendre et de connaître les conditions dans lesquelles un traitement de données à caractère personnel ayant pour objet l'évaluation ou l'analyse des pratiques de soins et de prévention doit être mis en œuvre pour respecter les dispositions de la loi.

ES25. La formation permet de comprendre et de connaître les garanties que doit présenter à la commission le responsable d'un traitement ayant pour objet l'évaluation ou l'analyse des pratiques de soins et de prévention.

ES26. La formation permet de comprendre et de connaître les conditions de sécurité à mettre en œuvre pour garantir la confidentialité des informations traitées par le traitement considéré, qu'il relève du chapitre IX ou X.

3.6. *Exigences relatives à la présentation du pouvoir de contrôle* a posteriori *de la CNIL*

ES27. La formation permet de comprendre et de connaître les différentes formes de contrôles *a posteriori* pouvant être effectués par la CNIL.

ES28. La formation permet de comprendre et de connaître le formalisme associé à une procédure de contrôle.

ES29. La formation permet de comprendre et de connaître les modalités pratiques d'exercice d'une procédure de contrôle.

ES30. La formation permet de comprendre et de connaître les droits et les obligations du responsable de traitements et des représentants de la CNIL dans le cadre d'une procédure de contrôle.

ES31. La formation permet de comprendre et de connaître les suites consécutives à un contrôle.

3.7. *Exigences relatives à la présentation du pouvoir de sanction de la CNIL*

ES32. La formation permet de comprendre et de connaître les différentes procédures de sanction pouvant être mises en œuvre par la CNIL.

ES33. La formation permet de comprendre et de connaître le fonctionnement de la commission réunie en formation restreinte et le déroulement d'une séance.

ES34. La formation permet de comprendre et de connaître le formalisme associé à une procédure de sanction, les droits et les obligations du responsable de traitement mis en cause et les voies de recours.

ES35. La formation permet de comprendre et de connaître les conditions de publication et de publicité des sanctions.

3.8. *Exigences relatives à la présentation des dispositions pénales associées au non-respect de la loi informatique et libertés*

ES36. La formation permet de comprendre et de connaître les conditions dans lesquelles un délit d'entrave à l'action de la CNIL est constitué.

ES37. La formation permet de comprendre et de connaître les sanctions pénales liées au non respect des exigences relatives au caractère loyal et licite de la collecte de données.

ES38. La formation permet de comprendre et de connaître les sanctions pénales relatives aux atteintes aux droits d'accès, de rectification ou d'opposition de la personne.

ES39. La formation permet de comprendre et de connaître les sanctions pénales liées au non-respect des exigences relatives à l'information des personnes.

ES40. La formation permet de comprendre et de connaître les sanctions pénales liées au non-respect des exigences relatives aux formalités préalables.

ES41. La formation permet de comprendre et de connaître les sanctions pénales liées au non-respect des exigences relatives à la sécurité des données.

ES42. La formation permet de comprendre et de connaître les sanctions pénales liées au non-respect des exigences relatives à la durée de conservation des données.

ES43. La formation permet de comprendre et de connaître les sanctions pénales liées au non-respect de la finalité des traitements.

ES44. La formation permet de comprendre et de connaître les sanctions pénales liées au non-respect des exigences relatives au traitement des données sensibles.