

Délégué à la protection des données (DPO)

RNCP35086 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326, 128
Formacode(s)	31045
Code(s) ROME	K1903
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	18/11/2020
Date d'échéance	18/11/2023

Certificateur(s)

DORANCO ESPACE MULTIMEDIA · SIRET : 38935885400054

Partenaires habilités

3 organismes habilités, d'après la liste publiée par France compétences : 3 à former.

Organisme	SIRET	Habilitation
AP FORMATION	44427438500020	Former
GROUPE GEMA - ESI BUSINESS SCHOOL / IA SCHOOL	82955681000028	Former
ICADEMIE	48908897100093	Former

Résumé de la certification

OBJECTIFS ET CONTEXTE

L'objectif de la certification est de former au métier de délégué à la protection des données (DPO) pour répondre aux besoins croissants des entreprises.

Ce métier est apparu suite aux évolutions majeures relatives aux obligations légales et à l'évolution de la réglementation liée à la protection des informations et de la vie privée et de la question de la sécurité des systèmes d'information.

Plus précisément, depuis le 25 mai 2018, date de mise en application dans tous les pays européens de ce règlement, toutes les entreprises publiques ou privées de plus de 250 salariés qui traitent des données sensibles à grande échelle ont l'obligation de nommer, au sein de leur organisation, une personne en charge de la sécurité et de la conformité des données. Il s'agit du rôle du délégué à la protection des données (DPO) ou data protection officer, tel que le définit l'article 37 du règlement général sur la protection des données (RGPD).

Même si l'article 37 précise que la nomination d'un DPO est obligatoire pour les structures de plus de 250 salariés, la commission nationale de l'informatique et des libertés (CNIL) recommande fortement la nomination d'un DPO quelle que soit la taille de la structure (entreprise, association ou collectivités locales), à noter que pour les petites structures, un DPO peut être indépendant et s'occuper de la protection des données personnelles de plusieurs sociétés, de manière mutualisée.

Le DPO est le successeur naturel du correspondant informatique et libertés (CIL), car sa mission est comparable. Néanmoins, les prérogatives du DPO sont renforcées, puisque le DPO dispose désormais de fonctions de conseil et de sensibilisation quant aux obligations relatives à la protection des données personnelles, que n'avait pas le correspondant de la CIL.

Véritable chef d'orchestre de la conformité du traitement des données, le DPO, doit disposer de bonnes connaissances sur les aspects organisationnels, méthodologiques et techniques de la sécurité des systèmes d'information.

ACTIVITÉS VISÉES

Le délégué à la protection des données ou data protection officer (DPO) est une personne nommée dont la mission principale consiste à garantir le respect de la protection des informations à caractère personnel. Pour cela, il intervient sur les mécanismes de traitement et de stockage des données de l'entreprise en lien avec le service informatique et les autres départements concernés (RH, marketing etc) afin de concevoir et mettre en place une politique de conformité du traitement des données à caractère sensible.

Maîtrisant parfaitement tous les éléments du règlement n° 2016/679, dit règlement général sur la protection des données (RGPD), il réalise un diagnostic de la conformité de son organisation. Il élabore puis met en place une politique de protection des données personnelles, veille au respect des obligations légales. Pour cela, il cartographie les catégories de données à sécuriser pour répondre aux exigences de la législation en cours puis crée et alimente un registre de traitement des données.

Disposant de solides compétences autour de la sécurité des systèmes d'information (SI), il conçoit aux côtés de la direction informatique et juridique, un système de management des données à caractère personnel (SMDCP) puis participe à la mise en œuvre de ce système dans le respect de la loi et des normes de sécurité.

Il est garant des questions de conservation, d'archivage, d'anonymisation et d'exploitation des données. D'autre part, ses connaissances dans le domaine de la cybersécurité lui permettent de proposer un plan de gestion de crise en cas de piratage des données, en coopération avec la direction informatique de son organisation. Il doit alors informer les personnes concernées de la perte de leurs données et jouer alors un rôle de médiateur auprès du public. Enfin, il assure la relation avec la commission nationale de l'informatique et des libertés (CNIL) et coordonne la réponse en cas de contrôle.

Ses activités principales sont:

- La conception d'une politique de conformité dans le respect du cadre légal « informatique et libertés »
- La mise en œuvre d'un système de management organisationnel et technique du traitement des données
- L'évaluation et gestion des risques liés aux données personnelles

COMPÉTENCES ATTESTÉES

Nous avons listé 18 compétences organisées en trois blocs de compétences :

Bloc de compétences " Conception d'une politique de conformité dans le respect du cadre légal « informatique et libertés »"

1-Effectuer un audit préliminaire de conformité légale et réglementaire de l'organisation, en collectant toutes les données nécessaires afin de révéler le niveau de risques afférant à chaque non-conformité

2-Rédiger un rapport de synthèse de l'audit préliminaire en cartographiant les traitements existants de données personnelles afin de sensibiliser les différents acteurs de l'organisation, de l'obligation de recensement et des risques ;

3-Créer et tenir le registre de traitements et de conservation des données afin de lister l'ensemble des processus de traitement des données personnelles en rassemblant une preuve pour chacun des processus ;

4-Créer une politique de gestion des données personnelles en listant les modalités de traitements des données personnelles afin d'informer les personnes concernées (salariés, clients, consommateurs ...) de leurs droits et des procédures de mise en œuvre de ces droits ;

5-Gérer les risques en réalisant une étude d'impact sur la protection des données afin de mettre en place un dispositif d'alertes (« Privacy impact assessment ») ;

Bloc de compétences "Mise en œuvre d'un système de management organisationnel et technique du traitement des données"

6-Répondre aux demandes externes en s'appuyant sur un processus de traitement des réclamations de personnes, relatives à l'exercice de leurs droits, afin de répondre rapidement aux sollicitations des personnes concernées et éviter les contentieux ;

7-Désigner les responsables de traitement internes ou externes et les sous-traitants afin de formaliser par écrit les relations entre les acteurs traitant les données, leurs rôles et responsabilités ;

8-Conduire un projet lié à la protection des données en définissant l'organisation et la planification du projet afin de réussir la conduite du changement ;

9-Animer des sessions de formation et de sensibilisation des collaborateurs au cadre légal « informatique et libertés », afin de responsabiliser les équipes et définir les nouveaux rôles transverses des personnes concernées ;

- 10-Organiser la protection des données dès la conception informatique d'un traitement (« Privacy By design ») en participant aux réunions de conception pour anticiper les risques de non-conformité ;
- 11-Piloter le système de management des données à caractère personnel (SMDCP) en disposant d'indicateurs afin de produire un bilan annuel de l'activité ;
- Bloc de compétences "Évaluation et gestion des risques liés aux données personnelles"
- 12-Établir une politique de sécurité informatique, en coordination avec les acteurs concernés (direction informatique) en déterminant notamment les données qui doivent relever d'une anonymisation ou d'une pseudonymisation afin de garantir la protection des données personnelles (« Privacy by default ») ;
- 13-Établir un plan de gestion de crise en cas de piratage des données en lien avec la direction informatique afin d'informer les personnes concernées des éventuelles diffusions de leurs données personnelles ;
- 14-Évaluer et gérer les risques dans le cadre d'un transfert de données hors Union européenne (UE) en utilisant les instruments juridiques de transfert adaptés ;
- 15-Renseigner et transmettre les formulaires de déclaration et/ou de demande d'autorisation délivrées par la CNIL afin d'informer la CNIL des éventuels risques liés au traitement ;
- 16-Gérer un audit de la CNIL en coopérant avec les autorités de contrôle concernées, afin de faciliter le processus interne de réponses à leurs sollicitations ;
- 17-Mettre à jour régulièrement le registre de traitement afin de répondre aux consignes et évolutions notifiées par la CNIL, en mettant en place préalablement, un plan d'actions correctives, le cas échéant ;
- 18-Réaliser une veille permanente sur son domaine d'activité en suivant la législation nationale, européenne et internationale afin de faire évoluer les pratiques internes le cas échéant ;

Blocs de compétences

RNCP35086BC01 — Conception d'une politique de conformité dans le respect du cadre légal « informatique et libertés »

LISTE DE COMPÉTENCES

- C1-1-Effectuer un audit préliminaire de conformité légale et réglementaire de l'organisation, en collectant toutes les données nécessaires afin de révéler le niveau de risques afférant à chaque non-conformité
- C1-2-Rédiger un rapport de synthèse de l'audit préliminaire en cartographiant les traitements existants de données personnelles afin de sensibiliser les différents acteurs de l'organisation, de l'obligation de recensement et des risques
- C1-3-Créer et tenir le registre de traitements et de conservation des données afin de lister l'ensemble des processus de traitement des données personnelles en rassemblant une preuve pour chacun des processus
- C1-4-Créer une politique de gestion des données personnelles en listant les modalités de traitements des données personnelles afin d'informer les personnes concernées (salariés, clients, consommateurs ...) de leurs droits et des procédures de mise en œuvre de ces droits
- C1-5-Gérer les risques en réalisant une étude d'impact sur la protection des données afin de mettre en place un dispositif d'alertes (« Privacy impact assessment »)

MODALITÉS D'ÉVALUATION

L'évaluation

du bloc est composée de deux volets :

- 1/ Une évaluation certificative finale du bloc devant un Jury composé de 2 professionnels extérieurs et en présence d'un membre du corps pédagogique
- Il s'agit d'une mise en situation professionnelle simulée consistant en la présentation de la mise en place d'un audit de conformité et d'une étude d'impacts sur la vie privée (EIVP).
- 2/ Plusieurs épreuves formatives* de type contrôles continus (*sauf pour les candidats en VAE)

RNCP35086BC02 — Mise en œuvre d'un système de management organisationnel et technique du traitement des données

LISTE DE COMPÉTENCES

- C2-1-Répondre aux demandes externes en s'appuyant sur un processus de traitement des réclamations de personnes, relatives à l'exercice de leurs droits, afin de répondre rapidement aux sollicitations des personnes concernées et éviter les contentieux
- C2-2-Désigner les responsables de traitement internes ou externes et les sous-traitants afin de formaliser par écrit les relations entre les acteurs traitant les données, leurs rôles et responsabilités

C2-3-Conduire un projet lié à la protection des données en définissant l'organisation et la planification du projet afin de réussir la conduite du changement

C2-4-Animer des sessions de formation et de sensibilisation des collaborateurs au cadre légal « informatique et libertés », afin de responsabiliser les équipes et définir les nouveaux rôles transverses des personnes concernées

C2-5-Organiser la protection des données dès la conception informatique d'un traitement (« Privacy By design ») en participant aux réunions de conception pour anticiper les risques de non-conformité

C2-6-Piloter le système de management des données à caractère personnel (SMDCP) en disposant d'indicateurs afin de produire un bilan annuel de l'activité

MODALITÉS D'ÉVALUATION

L'évaluation

du bloc est composée de deux volets :

1/ Une évaluation certificative finale du bloc devant un Jury composé de 2 professionnels extérieurs et en présence d'un membre du corps pédagogique

Il s'agit d'une mise en situation professionnelle simulée consistant en la description d'un système de management des données à caractère personnel (SMDCP)

2/ Plusieurs épreuves formatives* de type contrôles continus (*sauf pour les candidats en VAE)

RNCP35086BC03 — Évaluation et gestion des risques liés aux données personnelles

LISTE DE COMPÉTENCES

C3-1-Établir une politique de sécurité informatique, en coordination avec les acteurs concernés (direction informatique) en déterminant notamment les données qui doivent relever d'une anonymisation ou d'une pseudonymisation afin de garantir la protection des données personnelles (« Privacy by default »)

C3-2-Établir un plan de gestion de crise en cas de piratage des données en lien avec la direction informatique afin d'informer les personnes concernées des éventuelles diffusions de leurs données personnelles

C3-3-Évaluer et gérer les risques dans le cadre d'un transfert de données hors Union européenne (UE) en utilisant les instruments juridiques de transfert adaptés

C3-4-Renseigner et transmettre les formulaires de déclaration et/ou de demande d'autorisation délivrées par la CNIL afin d'informer la CNIL des éventuels risques liés au traitement

C3-5-Gérer un audit de la CNIL en coopérant avec les autorités de contrôle concernées, afin de faciliter le processus interne de réponses à leurs sollicitations

C3-6-Mettre à jour régulièrement le registre de traitement afin de répondre aux consignes et évolutions notifiées par la CNIL, en mettant en place préalablement, un plan d'actions correctives, le cas échéant

C3-7-Réaliser une veille permanente sur son domaine d'activité en suivant la législation nationale, européenne et internationale afin de faire évoluer les pratiques internes le cas échéant

MODALITÉS D'ÉVALUATION

L'évaluation

du bloc est composée de deux volets :

1/ Une évaluation certificative finale du bloc devant un Jury composé de 2 professionnels extérieurs et en présence d'un membre du corps pédagogique

Il s'agit d'une mise en situation professionnelle simulée consistant en la présentation d'un cas de transfert de données hors Union européenne (UE). Le candidat devra mettre à jour les registres de traitement ainsi que toutes les démarches auprès de la CNIL, après avoir vérifié la législation nationale et internationale.

2/ Plusieurs épreuves formatives* de type contrôles continus (*sauf pour les candidats en VAE)

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Tous les secteurs d'activités et toutes les entreprises, publiques ou privées mais aussi des associations reconnues d'utilité publique, qui gèrent des données de leurs clients, leurs abonnés, leurs salariés quels que soit le statut et la taille de la structure.

TYPE D'EMPLOIS ACCESSIBLES

- Délégué / Déléguée à la protection des données - Data Protection Officer
- Correspondant / Correspondante informatique et libertés - CIL
- Auditeur / Auditrice en sécurité des systèmes d'information

RÈGLEMENTATIONS D'ACTIVITÉ

L'exercice du métier de Délégué à la protection des données n'est pas réglementé mais ce professionnel travaille en s'appuyant sur un cadre réglementaire précis:

- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Il constitue le texte de référence en matière de protection des données personnelles. Ses dispositions sont directement applicables dans l'ensemble des États membres à compter du 25 mai 2018.
- La loi " Informatique et Libertés " du 6 janvier 1978 et la loi du 20 juin 2018 relative à la protection des données personnelles.
- Délibération n° 2018-318 du 20 septembre 2018 portant adoption des critères du référentiel de certification des compétences du délégué à la protection des données (DPO).

Marché du travail

Indicateurs au niveau des familles professionnelles (FAP) des métiers visés, agrégés au niveau national — France Travail / DARES (open data).

Tension de recrutement (DARES 2024)	Modérée (3/5)
Facteurs principaux	Lien formation-emploi, Manque de main-d'œuvre disponible
Salaire médian (mensuel)	2 600 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en sciences humaines et droit (58 % des actifs en emploi)
Familles professionnelles (FAP)	L5X91 — Juristes et avocats · tension 3/5 (Modérée)
Projets de recrutement (BMO 2026)	2 886
Jugés difficiles à recruter	38 %
Emplois saisonniers	6 %
Familles professionnelles (FAP)	L5X91 — Juristes et avocats

Voies d'accès

MODALITÉS D'ACCÈS

Formation continue, Apprentissage, Contrat de professionnalisation, Candidature individuelle, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

L'accès au titre est ouvert aux candidats titulaires d'un niveau 6 dans le domaine juridique ou la sécurité informatique. La formation exige aussi :

- o Un bon niveau de Français, à l'écrit et à l'oral ;
- o Une expérience d'une durée au moins d'un an dans le domaine juridique ou la sécurité informatique ;
- o Un goût prononcé pour les nouvelles technologies et la communication ;

Les prérequis sont vérifiés dans le cadre d'une évaluation diagnostique (tests d'entrée et étude de dossier) par notre équipe pédagogique.

Dérogation :Les candidats titulaires d'un diplôme de niveau 4 ou 5 peuvent demander une admission à titre dérogatoire à condition de justifier d'une expérience de 2 années minimum dans des projets, activités ou tâches en

lien avec les missions du DPO s'agissant de la protection des données personnelles.
Dans ce cas, ils doivent réussir les tests d'évaluation des connaissances et l'entretien de motivation.

COMPOSITION DU JURY — FORMATION CONTINUE, APPRENTISSAGE, CONTRAT DE PROFESSIONNALISATION, CANDIDATURE INDIVIDUELLE

3 personnes :

- Le référent pédagogique
 - 2 professionnels extérieurs
- soit 66% de membres extérieurs

COMPOSITION DU JURY — VAE

3 personnes :

- Le référent pédagogique
 - 2 professionnels extérieurs
- soit 66% de membres extérieurs

Financement en alternance (NPEC)

Niveau de prise en charge d'un contrat d'apprentissage par les OPCO, fixé par France compétences par branche professionnelle (CPNE).

Prise en charge usuelle	8 684 €
Selon la branche	7 500 € – 8 789 €

Prise en charge	Branches concernées
8 684 €	Valeur par défaut · 205 branches
8 789 €	CPNE FP Commerce de Détail de l'Horlogerie Bijouterie, CPNEFP ICGV entreprises de la viande
8 668 €	CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager, CPNEFP du Négoce de l'ameublement
8 752 €	CPNEFP dans les établissements d'enseignement privés sous contrat
8 700 €	CPNEFP des jardineries et graineteries
8 583 €	CPNEFP Commerce à distance
7 500 €	CPNE des industries de santé (CPNEIS)

Base légale

Date de décision	18/11/2020
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	18/11/2023

Liens avec d'autres certifications

NOUVELLE(S) CERTIFICATION(S)
RNCP41460

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://www.doranco.fr/formation/parcours/131-delegue-e-a-la-protection-des-donnees-data-protection-officer->

Fiche officielle (France Compétences)

Entrées et sorties de formation

Entrées en formation	4
Parcours menés à terme	4
Taux d'achèvement	100 %
Période	02/2022 – 08/2024

Entrées et sorties — Caisse des Dépôts (open data), tous organismes confondus.

Demande CPF — formations engagées

Dossiers CPF engagés	5
Montant total engagé	25 565 €
Coût moyen par dossier	5 113 €
Durée moyenne	600 h
Période	01/2022 – 08/2023
France compétences	72 %
France Travail	20 %
Entreprise	6 %
Reste à charge titulaire	1 %

Formations engagées via le CPF — Caisse des Dépôts (open data), tous organismes confondus.