

Délégué à la protection des données (DPO)

RNCP36448 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326p, 128
Formacode(s)	13238, 31006
Code(s) ROME	K1903, M1802
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	01/06/2022
Date d'échéance	01/06/2025

Certificateur(s)

ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE (AFINUM) · SIRET : 39350481600231

Partenaires habilités

20 organismes habilités, d'après la liste publiée par France compétences : 20 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE (AFINUM)	39350481600090	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE (AFINUM)	39350481600215	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE (AFINUM)	39350481600223	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE (AFINUM)	39350481600231	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE (AFINUM)	39350481600249	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE (AFINUM)	39350481600272	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE (AFINUM)	39350481600298	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE (AFINUM)	39350481600306	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE (AFINUM)	39350481600314	Former et organiser l'évaluation
ASSOCIATION POUR LA FORMATION A L'INFORMATIQUE ET AU NUMERIQUE (AFINUM)	39350481600322	Former et organiser l'évaluation

Liste complète des 20 partenaires habilités : <https://data.aktaconseil.fr/certifications/rncp36448-delegue-a-la-protection-des-donnees-dpo/partenaires>

Résumé de la certification

OBJECTIFS ET CONTEXTE

Cette certification a comme objectif de répondre à un besoin croissant en compétences dans le domaine de la protection des données.

Elle a été créée dans le contexte où

l'utilisation des données à caractère personnel de plus en plus généralisée et importante au sein des entreprises, a fait naître une nouvelle approche de la donnée via l'éthique de celle-ci. Ainsi, avec cette approche et sous l'impulsion du RGPD, la fonction de délégué à la protection des données (DPO) a émergé et est aujourd'hui demandée et exigée au sein des entreprises et organisations utilisant des données à caractère personnel.

ACTIVITÉS VISÉES

Activité 1 : Définition de la politique de la protection de données personnelle en accord avec la stratégie de l'entreprise et dans le respect du cadre législatif

A1T1- Analyse du système d'information de l'entreprise

dans le cadre de la protection des données personnelles

A1T2- Cadrage réglementaire lié à la protection de données personnelles (RGPD)

Activité 2 : Pilotage du projet de conformité réglementaire liée à la protection de données

A2T1.Organisation des actions spécifiques au projet de conformité réglementaire liée à la protection des données

A2T2. Conception de la stratégie du projet de conformité réglementaire liée à la protection de données

Activité 3 :

Déploiement et règlement général sur la protection des données au sein de la structure

A3T1 Conception des mesures de sécurité informatique pour les données à caractère personnelle

A3T2 La gestion des documents juridiques dans le contexte du RGPD

Activité 4 : Amélioration continue de la stratégie de mise en conformité réglementaire RGPD

A4T1 Sensibilisation des collaborateurs pour la protection des données

A4T2 Amélioration continue de la stratégie de mise en conformité réglementaire liée à la RGPD

COMPÉTENCES ATTESTÉES

A1C1. Analyser le système d'information (SI) existant au sein de la structure dans son intégralité, selon une méthode d'analyse adaptée, afin de pouvoir en tirer un diagnostic sur le système étudié

A1C2. Identifier les rôles et responsabilités de chacun au sein de l'organisation en lien avec la politique de protection des données établie afin de définir un plan de communication sur le projet adapté

A1C3. Réaliser un diagnostic organisationnel de la structure afin de clarifier les objectifs de la protection des données

A1C4. Etablir les enjeux techniques, juridiques, financiers et éthiques de la structure, en lien avec les différents services, afin d'assurer une stratégie de protection des données conforme et cohérente.

A1C5. Définir la politique de protection des données adaptée aux contraintes structurelles, organisationnelles de la structure, afin que le SI soit en accord avec les règles de protection des données en vigueur

A1C6. Restituer auprès de la direction et des différentes direction métiers le diagnostic du système de l'entreprise afin de faire valider par les décisionnaires la politique de protection des données choisies et d'impliquer les différents acteurs

A2C1.Déterminer les actions spécifiques du projet de conformité réglementaire afin de pouvoir les ordonner et les prioriser, à travers une feuille de route (roadmap)

A2C2.Définir la méthode de gestion de projet adaptée à mettre en œuvre afin de gagner en efficacité pendant le déploiement du projet de conformité réglementaire et de veiller à réduire les écarts avec le cadre législatif en vigueur

A2C3.Décomposer le projet en grande séquence afin d'en déterminer les résultats attendus à chaque fin de séquence et ainsi, permettre d'en déduire les indicateurs de suivi et de performance.

A2C4.Repérer les risques (techniques et humains) en amont du projet afin d'en maîtriser les impacts à court terme.

A2C5. Adopter une stratégie d'accueil aux handicaps afin de favoriser l'inclusion des profils en situation de handicap au sein de l'équipe et permettre leur pleine intégration, en collaboration avec le référent handicap de l'entreprise

A2C6.Etablir le planning global du projet afin d'organiser la mise en œuvre du projet en tenant compte des contraintes de délais, de coûts et de moyens du projet.

A2C7. Cartographier Les flux en indiquant l'origine et la destination des données, afin notamment d'identifier les éventuels transferts de données hors de l'Union européenne

A2C8.

Déployer un registre de traitement de données personnelles de la structure afin de recenser de façon précise les différents traitements de données personnelles de la structure et de le transmettre, le cas échéant, à la CNIL

A2C9. Définir une structure organisationnelle de protection des données en interne, en identifiant pour chaque direction métier, une personne relais afin de sécuriser la politique de protection des données qui sera mise en œuvre

A2C10. Identifier les acteurs externes qui traitent les données personnelles, en précisant clairement les prestataires sous-traitants afin d'actualiser les clauses de confidentialité

A2C11. Etablir la liste des actions prioritaires à partir de l'analyse des risques en s'appuyant sur le du registre de traitements des données afin de rendre ses traitements conforme à la réglementation et ainsi sécuriser les risques sur les droits et les libertés des personnes concernées

A3C1. Auditer les mesures existantes mise en place pour la sécurité des données au sein de la structure afin de mettre en évidence les dysfonctionnement et anomalies du SI existant

A3C2. Déployer les mesures de sécurité applicative et système en proposant des solutions techniques innovantes pour le système d'information en commun accord avec le responsable de la sécurité du S.I (RSSI) de la structure afin de traiter chaque risque de façon spécifique et ainsi garantir la conformité réglementaire

A3C3. Concevoir les procédures internes en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement des données afin d'installer des bonnes pratiques d'utilisation de données et veiller à leurs applications par les différentes direction métiers

A3C4. Effectuer une veille constante dans le domaine technique, légale et juridique sur la protection des données, afin de pouvoir déterminer des actions de rectification par rapport aux nouvelles techniques ou lois et assurer ainsi la conformité du traitement des données à caractère personnel

A3C5. Collecter la documentation juridique en lien avec la réglementation RGPD afin de constituer une base documentaire juridique utile et ainsi répondre, le cas échéant, aux sollicitations de la CNIL en se basant sur des éléments de preuves législatives

A3C6. Élaborer un plan de communication interne pour informer l'ensemble des employés de la structure de son rôle en tant que DPO, de son statut et de ses futurs plans d'action

A4C1 Concevoir une campagne de sensibilisation afin d'informer l'ensemble des collaborateurs et d'initier une réflexion globale sur la protection des données à caractère personnel dans la structure

A4.C2 Former les publics cibles à l'aide de contenus thématiques adapté afin de les guider dans l'appropriation des procédures RGPD mis en place par la structure

A4.C3 Réaliser des présentations orales à l'aide d'un support visuel pour des publics cibles en interne afin de les informer sur le RGPD et d'en faciliter l'acceptation.

A4.C4 Concevoir

des supports adaptés aux personnes en situation de handicap

afin de permettre à tout public d'accéder librement et facilement au numérique (public cible, collaborateurs interne, sous-traitants ...)

A4.C5 Appliquer les procédures d'audits de sécurité informatiques périodiques afin d'ajuster la politique de sécurité des données de façon régulière et le cas échéant, de donner lieu à un plan d'action correctif

A4.C6 Contrôler la bonne application des mesures de la protection des données afin de vérifier leurs applications opérationnelles par les différents acteurs et alerter les directions métiers en cas de non-respect des procédures de sécurité des données

A4.C7 Mutualiser l'expérience et les difficultés avec des DPO du même secteur afin de diffuser plus largement les solutions et les bonnes pratiques

Blocs de compétences

RNCP36448BC01 — Elaborer le cadre juridique RGPD et protection des données de l'entreprise

LISTE DE COMPÉTENCES

1. Réaliser un diagnostic organisationnel de la structure afin de clarifier les objectifs de la protection des données
2. Restituer auprès de la direction et des différentes direction métiers le diagnostic du système de l'entreprise afin de faire valider par les décideurs la politique de protection des données choisies et d'impliquer les différents acteurs
3. Etablir les enjeux techniques, juridiques, financiers et éthiques de la structure, en lien avec les différents services, afin d'assurer une stratégie de protection des données conforme et cohérente.
4. Identifier les acteurs externes qui traitent les données personnelles, en précisant clairement les prestataires sous-

traitants afin d'actualiser les clauses de confidentialité

5. Collecter la documentation juridique en lien avec la réglementation RGPD afin de constituer une base documentaire juridique utile et ainsi répondre, le cas échéant, aux sollicitations de la CNIL en se basant sur des éléments de preuves législatives

6. Déployer un registre de traitement de données personnelles de la structure afin de recenser de façon précise les différents traitements de données personnelles de la structure et de le transmettre, le cas échéant, à la CNIL

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle reconstituée

A partir d'un cahier des charges d'une entreprise fictive, établi par l'organisme certificateur précisant les besoins d'une entreprise fictive, le candidat doit définir les objectifs de la protection de données personnelles, rédiger un diagnostic organisationnel, réaliser un document clair et précis présentant une politique de protection de données personnelles et la présenter oralement, lister les enjeux

enjeux techniques, juridiques, financiers et éthiques de l'entreprise, rédiger une synthèse, présenter un document détaillant les différents acteurs externes en lien avec les données personnelles, les documents juridiques liés au RGPD et un registre des traitements de données

RNCP36448BC02 — Déployer une stratégie de protection des données

LISTE DE COMPÉTENCES

1. Analyser le système d'information (SI) existant au sein de la structure dans son intégralité, selon une méthode d'analyse adaptée, afin de pouvoir en tirer un diagnostic sur le système étudié
2. Définir la politique de protection des données adaptée aux contraintes structurelles, organisationnelles de la structure, afin que le SI soit en accord avec les règles de protection des données en vigueur
3. Cartographier Les flux en indiquant l'origine et la destination des données, afin notamment d'identifier les éventuels transferts de données hors de l'Union européenne
4. Auditer les mesures existantes mise en place pour la sécurité des données au sein de la structure afin de mettre en évidence les dysfonctionnement et anomalies du SI existant
- 5.

Etablir la liste des actions prioritaires à partir de l'analyse des risques en s'appuyant sur le registre de traitements des données afin de rendre ses traitements conforme à la réglementation et ainsi sécuriser les risques sur les droits et les libertés des personnes concernées

6. Concevoir les procédures internes en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement des données afin d'installer des bonnes pratiques d'utilisation de données et veiller à leurs applications par les différentes directions métiers

7. Déployer les mesures de sécurité applicative et système en proposant des solutions techniques innovantes pour le système d'information en commun accord avec le responsable de la sécurité du S.I (RSSI) de la structure afin de traiter chaque risque de façon spécifique et ainsi garantir la conformité réglementaire

8. Contrôler la bonne application des mesures de la protection des données afin de vérifier leurs applications opérationnelles par les différents acteurs et alerter les directions métiers en cas de non-respect des procédures de sécurité des données

9. Appliquer les procédures d'audits de sécurité informatiques périodiques afin d'ajuster la politique de sécurité des données de façon régulière et le cas échéant, de donner lieu à un plan d'action correctif

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle reconstituée

A partir d'un cahier des charges, établi par l'organisme certificateur précisant les besoins d'une entreprise fictive, le candidat doit analyser le système d'information, définir une politique de la protection des données personnelles adaptée au contexte de l'entreprise,

présenter un document détaillant pour chaque traitement de données

l'origine, la destination, les acteurs,

une synthèse d'un audit de sécurité du SI en proposant un plan d'actions suite à une analyse d'impacts relatifs à la protection de données, rédiger des procédures internes pour assurer la sécurité des données et

des solutions de sécurité de SI à mettre en place, présenter un état d'avancement des mesures mises en place et un processus permanent d'Audit de sécurité Informatique

RNCP36448BC03 — Manager un projet de protection de données

LISTE DE COMPÉTENCES

1. Identifier les rôles et responsabilités de chacun au sein de l'organisation en lien avec la politique de protection des données établie afin de définir un plan de communication sur le projet adapté
2. Définir une structure organisationnelle de protection des données en interne, en identifiant pour chaque direction métier, une personne relais afin de sécuriser la politique de protection des données qui sera mise en œuvre
3. Repérer les risques (techniques et humains) en amont du projet afin d'en maîtriser les impacts à court terme.
4. Déterminer les actions spécifiques du projet de conformité réglementaire afin de pouvoir les ordonner et les prioriser, à travers une feuille de route (roadmap)
5. Définir la méthode de gestion de projet adaptée à mettre en œuvre afin de gagner en efficacité pendant le déploiement du projet de conformité réglementaire et de veiller à réduire les écarts avec le cadre législatif en vigueur
6. Décomposer le projet en grande séquence afin d'en déterminer les résultats attendus à chaque fin de séquence et ainsi, permettre d'en déduire les indicateurs de suivi et de performance.
7. Adopter une stratégie d'accueil aux handicaps afin de favoriser l'inclusion des profils en situation de handicap au sein de l'équipe et permettre leur pleine intégration, en collaboration avec le référent handicap de l'entreprise
8. Etablir le planning global du projet afin d'organiser la mise en œuvre du projet en tenant compte des contraintes de délais, de coûts et de moyens du projet.

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle reconstituée

A partir d'un cahier des charges, établi par l'organisme certificateur précisant les besoins d'une entreprise fictive, le candidat doit définir un organigramme fonctionnel avec le rôle de chaque ressource dans la mise en place d'une politique de protection de données et présenter la méthode de gestion de projet inclusif adaptée à la mise en place de la politique de protection de données personnelles et les ressources du projet en détaillant les différentes étapes du projet et en présentant une analyse des risques du projet

RNCP36448BC04 — Accompagner les directions métiers et les collaborateurs dans la mise en œuvre de la stratégie de protection des données

LISTE DE COMPÉTENCES

1. Effectuer une veille constante dans le domaine technique, légale et juridique sur la protection des données, afin de pouvoir déterminer des actions de rectification par rapport aux nouvelles techniques ou lois et assurer ainsi la conformité du traitement des données à caractère personnel
2. Élaborer un plan de communication interne pour informer l'ensemble des employés de la structure de son rôle en tant que DPO, de son statut et de ses futurs plans d'action
3. Concevoir une campagne de sensibilisation afin d'informer l'ensemble des collaborateurs et d'initier une réflexion globale sur la protection des données à caractère personnel dans la structure
4. Former les publics cibles à l'aide de contenus thématiques adaptés afin de les guider dans l'appropriation des procédures RGPD mis en place par la structure
5. Réaliser des présentations orales à l'aide d'un support visuel pour des publics cibles en interne afin de les informer sur le RGPD et

d'en faciliter l'acceptation.

6. Concevoir

des supports adaptés aux personnes en situation de handicap

afin de permettre à tout public d'accéder librement et facilement au numérique (public cible, collaborateurs interne, sous-traitants ...)

7. Mutualiser l'expérience et les difficultés avec des DPO

du même secteur afin de diffuser plus largement les solutions et les bonnes pratiques

MODALITÉS D'ÉVALUATION

Mise en situation professionnelle reconstituée

A partir d'un cahier des charges, établi par l'organisme certificateur précisant les besoins d'une entreprise fictive, le candidat doit présenter un process de veille dans le domaine de la protections des données personnelles, le candidat doit présenter un plan de communication sur le rôle du DPO et ses plans d'actions,

une compagne de sensibilisation sur la protection des données personnelles, un exemplaire d'une fiche de formation sur la réglementation RGPD, une ébauche de présentation générale d'une procédure RGPD, des supports de communication tenant en compte d'un public à situation de handicap et une synthèse des réseaux utiles identifiés et un process d'échange sur la conformité réglementaire

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Le DPO peut exercer ses fonctions au sein soit du service de traitement des données, soit en tant que sous-traitant indépendant ou faisant parti d'associations et autres organismes représentant des responsables du traitement ou des sous-traitants.

Le DPO peut donc intégrer le service de traitement des données et dépend dans ce cas-là du responsable de traitement des données

Le DPO peut donc être amené à exercer dans tous les secteurs d'activités existants et au sein de tous types de structures telles que :

- Une entreprise privée dont l'activité de base les amène à réaliser un suivi régulier et systématique des personnes à grande échelle, ou à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et infractions.
- En intégrant le service de traitement des données, sous la hiérarchie du responsable de traitement des données
- En tant que sous-traitant indépendant ou faisant parti d'associations et autres organismes représentant des responsables du traitement ou des sous-traitants.
- Un organisme public ou autorité publique (indépendamment de la nature des données qu'ils traitent)

TYPE D'EMPLOIS ACCESSIBLES

Pour assurer cette fonction, selon les entreprises et organisations, il existe différents types d'emplois qui sont les suivants :

- Data Protection Officer (DPO)
- Délégué à la Protection des Données (DPD)
- Data Protection Manager/Specialist
- Consultant RGPD
- Chargé de mission Données Personnelles/Protection des Données
- Consultant Données à Caractère Personnel Relais Informatique et Libertés

Nous trouvons les différents intitulés d'emploi dans les analyses effectuées sur les 821 offres d'emploi

RÈGLEMENTATIONS D'ACTIVITÉ

Il n'existe pas de réglementation d'activité ou de dépendance avec une convention ou une réglementation concernant le métier de DPO. En revanche, dans l'exercice de ses fonctions et pour la bonne réalisation de ses missions, le DPO devra prendre en compte ;

- Le RGPD, Chapitre IV, Section 4 ;
- La 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) ;
- La loi « Informatique et Libertés » du 6 janvier 1978 et la loi du 20 juin 2018 relative à la protection des données

personnelles.

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)	Élevée (4/5) Moyenne pondérée par l'emploi ; les familles ci-dessous s'échelonnent de 3 à 5 sur 5.
Facteurs principaux	Lien formation-emploi, Manque de main-d'œuvre disponible
Salaire médian (mensuel)	2 893 €
Diplôme le plus fréquent	Diplôme de niveau bac+5 ou plus (doctorat, master ou équivalent) en communication et information (35 % des actifs en emploi)
Familles professionnelles (FAP)	L5X91 — Juristes et avocats · tension 3/5 (Modérée) M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée)
Projets de recrutement (BMO 2026)	7 644
Jugés difficiles à recruter	42 %
Emplois saisonniers	2 %
Familles professionnelles (FAP)	L5X91 — Juristes et avocats M2X93 — Experts et consultants en systèmes d'information

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

La formation est accessible aux :

1- en Formation initiale ou par alternance : Titulaires d'un diplôme (licence professionnelle) ou d'une certification professionnelle RNCP de niveau 6 en informatique en Informatique/ sécurité informatique et ou en droit informatique/ droit en propriété intellectuelle. Pour ces candidats, l'accès au dispositif de certification est le suivant : passage de tests de connaissances et de compétences suivis d'un entretien de motivation.

ou

2- Salariés

des entreprises du secteur numérique et ou juridique ; .Jeunes de 19 à 26 ans et adultes demandeurs d'emplois de plus de 26 ans

possédant : un diplôme de niveau 5

(BTS/DUT) ou une certification de niveau 5 en informatique / sécurité informatique et ou en droit informatique/ droit en propriété intellectuelle avec une expérience professionnelle d'au moins un an dans un métier informatique ou en droit informatique

Ou un diplôme

(licence professionnelle) ou une certification professionnelle RNCP de niveau 6 en informatique ou en droit informatique

Pour ces candidats, l'accès au dispositif de la certification est le suivant : tests d'auto-positionnement (tests de compétences) suivis d'un entretien individualisé (entretien de positionnement) afin de proposer un parcours de formation adapté selon les expériences acquises auparavant.

Ou

3- Personnes en reconversion professionnelle : sur examen du dossier en fonction des acquis professionnels et des expériences professionnelles antérieures.

Pour ces candidats, l'accès au dispositif de la certification est le suivant : tests d'auto-positionnement (tests de compétences) suivis d'un entretien individualisé (entretien de positionnement) afin de proposer un parcours de formation adapté selon les expériences acquises auparavant.

COMPOSITION DU JURY — FORMATION INITIALE

Le président

du jury est un professionnel extérieur à l'organisme de formation et est désigné par l'ensemble des membres du jury. Le jury se compose de trois personnes :

- Deux membres externes professionnels (employeur ou salarié de métier délégué à la protection des données (Professionnels du secteur non intervenant au sein du parcours de formation préparant à la certification).

L'un de ces deux membres est président du jury ;

- Un membre de la Direction de l'innovation et de la pédagogie de l'organisme certificateur ou son représentant/sa représentante qui peut être : le Directeur ou le Responsable pédagogique du campus EPSI régional auquel est rattaché le candidat

COMPOSITION DU JURY — FORMATION CONTINUE

Le président

du jury est un professionnel extérieur à l'organisme de formation et est désigné par l'ensemble des membres du jury. Le jury se compose de trois personnes :

- Deux membres externes professionnels (employeur ou salarié de métier délégué à la protection des données (Professionnels du secteur non intervenant au sein du parcours de formation préparant à la certification).

L'un de ces deux membres est président du jury ;

- Un membre de la Direction de l'innovation et de la pédagogie de l'organisme certificateur ou son représentant qui peut être : le Directeur ou le Responsable pédagogique du campus EPSI régional auquel est rattaché le candidat.

COMPOSITION DU JURY — APPRENTISSAGE

Le président

du jury est un professionnel extérieur à l'organisme de formation et est désigné par l'ensemble des membres du jury. Le jury se compose de trois personnes :

- Deux membres externes professionnels (employeur ou salarié de métier délégué à la protection des données (Professionnels du secteur non intervenant au sein du parcours de formation préparant à la certification).

L'un de ces deux membres est président du jury ;

- Un membre de la Direction de l'innovation et de la pédagogie de l'organisme certificateur ou son représentant qui peut être : le Directeur ou le Responsable pédagogique du campus EPSI régional auquel est rattaché le candidat

COMPOSITION DU JURY — CONTRAT DE PROFESSIONNALISATION

Le président

du jury est un professionnel extérieur à l'organisme de formation et est désigné par l'ensemble des membres du jury. Le jury se compose de trois personnes :

- Deux membres externes professionnels (employeur ou salarié de métier délégué à la protection des données (Professionnels du secteur non intervenant au sein du parcours de formation préparant à la certification).

L'un de ces deux membres est président du jury ;

- Un membre de la Direction de l'innovation et de la pédagogie de l'organisme certificateur ou son représentant qui peut être : le Directeur ou le Responsable pédagogique du campus EPSI régional auquel est rattaché le candidat.

COMPOSITION DU JURY — VAE

Le président

du jury est un professionnel extérieur à l'organisme de formation et est désigné par l'ensemble des membres du jury. Le jury se compose de trois personnes :

- Deux membres externes professionnels (employeur ou salarié de métier délégué à la protection des données (Professionnels du secteur non intervenant au sein du parcours de formation préparant à la certification). L'un de ces deux membres est président du jury ;

- Un membre de la Direction de l'innovation et de la pédagogie de l'organisme certificateur ou son représentant qui peut être : le Directeur ou le Responsable pédagogique du campus EPSI régional auquel est rattaché le candidat.

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

8 736 €

Selon la branche

7 000 € – 9 800 €

Prise en charge	Branches concernées
8 736 €	Valeur par défaut · 190 branches
8 696 €	CPNE FP Commerce de Détail de l'Horlogerie Bijouterie, CPNEFP Commerce succursaliste de la Chaussure, CPNEFP Commerce à distance, CPNEFP Grands Magasins/ Magasins Populaires, CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager
9 800 €	CPNE Casinos, CPNE autoroutes, CPNE de l'édition de livres, de l'édition phonographique et de l'édition de musique, CPNE des Télécoms, CPNEF de l'audiovisuel
9 005 €	CPNE FP Branche des magasins du Bricolage
9 000 €	CPNEFP de la Mutualité Sociale Agricole
8 974 €	CPNE de la branche de la Distribution Directe
8 813 €	CPNEFP Professions de la Photographie
8 775 €	CPNEFP de la branche des entreprises du bureau et du numérique (commerces et services)
8 600 €	CPNEFP de l'habillement, mercerie, chaussure et jouet
8 509 €	CPNEFP de la Branche des Caisses régionales de Crédit Agricole et autres organismes
7 697 €	CPNEFP de la blanchisserie, laverie, location de linge, nettoyage à sec, pressing et teinturerie
7 500 €	CPNE des industries de santé (CPNEIS)
7 000 €	CPNEFP de la métallurgie

Base légale

Date de décision	01/06/2022
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	01/06/2025

Liens avec d'autres certifications

NOUVELLE(S) CERTIFICATION(S)
RNCP41409

CORRESPONDANCES (PAR BLOCS)
RNCP32106

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/36448/>