Description

Formation de DPO : 5 jours - 35 Heures

- Formation permettant de valider le Bloc N° 2 de la Licence "Responsable de la protection des données des organisations" (RNCP 35680) (voir en fin de document)
- Formation de DPO permettant au stagiaire de présenter la Certification des Compétences de DPO (Référentiel CNIL)

Le programme se déroule sur 5 jours soit 35 heures de formation couvrant les 3 domaines de connaissance du DPO pour la Certification

- Réglementation
- Responsabilité
- Sécurité

Elle couvre également les 17 domaines de compétences attendus du DPO

Jour 1 : RGPD la règlementation
Jour 2 : Le DPO : rôle et responsabilité
Jour 3 : les Outils du DPO, méthode d'action
Jour 4 : Les Autorités de Contrôle, les Transferts de données
Jour 5 : Sécurité des Données à Caractère personnel et PIA

Les après-midi des JOURS, 2, 3, 4, 5 sont consacrés à la réalisation de cas pratiques.

Objectifs de la formation

Cette formation a pour objectif :

- de valider le Bloc N°2 de la licence Niv 6 "Responsable de la protection des données des organisations"
- de préparer le stagiaire et lui permettre de présenter l'examen de Certification de Compétences de DPO (ref CNIL)

Cette certification suit le référentiel publié par la CNIL le 11 octobre 2018 (NOR CNIL 1827457X)

A l'issue de la formation, le participant est en capacité de :

- Comprendre les enjeux de la protection des données et le cadre de la règlementation à un niveau très fin permettant de présenter la certification opérée par les organismes de certification agréés par la CNIL
- Connaitre les principes du RGPD et se les approprier dans un contexte professionnel, de diagnostic, de conseil, de DPO, de formation.
- Mettre en œuvre les outils de conformité RGPD dans son entreprise ou chez un tiers client
- Construire et maintenir les éléments de preuve de la conformité
- Conseiller les Responsables de Traitements sur la conduite et la gestion des études d'impacts sur la vie privée PIA (EIVP)
- Connaître les outils de suivi de la conformité
- Conseiller les responsables de traitement sur les principaux moyens de sécurisation de données personnelles

Il sera remis au stagiaire une attestation de suivi, un certificat et un bilan de formation.
Cette formation sanctionne l'obtention du BLOC N°2 de la LICENCE Niveau VI "Responsable de la protection des Données des Organisations" (RNCP 35680)

Public visé

oute personne (employé, professionnel libéral, demandeur d'emploi...) souhaitant acquérir les compétences nécessaires pour comprendre en profondeur la protection des données personnelles. Cette formation permet d'obtenir les prérequis pour passer l'examen de certification de Compétences de DPO selon le référentiel CNIL.

Cette formation permet de valider le Bloc N° 2 de la licence Niveau VI "Responsable de la protection des données des organisations"

Informations sur l'admission

Le processus d'admission inclus un questionnaire de recueil de besoins et d'appréciation du niveau du candidat, suivi, si besoin, par un entretien oral :

- niveau de diplôme ou équivalent permettant de suivre aisément la formation
- besoins de formations en fonction des connaissances initiales
- attentes vis à vis de la formation
- attente vis à vis de la certification

En cas de doute sur la capacité du candidat à suivre la formation nous invitons les entreprises et les futurs stagiaires à nous faire part de leur doutes et questions.

Délai pour l'admission à la formation

- **Via CPF**
  - Min.
    12 jours ouvrés entre votre demande via Mon Compte Formation et la date de début de session
- **Via France Travail**
  - Min. 3 semaines complètes entre la date de dépôt de votre devis sur Kairos et la date de début de la session
- **En Direct chez Impact RGPD**
  - Min. 2 jours ouvrés entre votre demande et la date de début de session

Modalités d'admission

- Admission sans disposition particulière

Prérequis

Pré-Requis pour la formation:
Pour suivre aisément notre formation de DPO, nous demandons à nos stagiaires d'être titulaires d'un diplôme niveau bac +2 ou supérieur ou équivalent en VAE .

La fonction de DPO nécessite d'avoir une bonne connaissance de l'entreprise, ses services, des notions de pratiques et d'organisation.

Au moment de votre inscription un questionnaire de recueil de besoins et d'entrée en formation vous sera remis et devra être complété.

Un entretien téléphonique avec Impact RGPD vous sera proposé et vous permettra de lever tout doute sur votre capacité à suivre la formation dans de bonnes conditions.

Si vous vous interrogez sur vos prérequis, contactez-nous pour nous faire part de votre expérience professionnelle.

Pré-requis pour l'examen de Certification de Compétences de DPO:

Pour passer la certification de Compétences de DPO selon le référentiel Cnil, les candidats devront :

- justifier d'une **expérience pro**fessionnelle d'au moins **2 ans**

Afin d'amener la preuve de la conformité aux prérequis le participant devra fournir tous les éléments nécessaires à l'établissement de la preuve à savoir (les éléments marqués d'un * sont obligatoires):

- Copie des diplômes obtenus
- Curriculum Vitae à date de la présente convention *

Ces documents
seront demandés par
l'Organisme qui fait passer l'examen au moment de l'inscription à l'examen.

Modalités pédagogiques

Formation en présentiel ou en distanciel sur 5 journées, soit 35 heures.
Modalités : animation pédagogique, travaux en groupe, cas pratiques, questions d'entrainement à la certification
La formation peut être suivie en présentiel comme en distanciel : ce choix est laissé au stagiaire

Moyens et supports pédagogiques

La formation utilise plusieurs ressources pédagogiques combinées.

- Des supports de formation (slides) commentées par l'animateur
- Des jeux de rôles réalisés en groupe
- Des tests et Quiz individuels d'évaluation des acquis et de préparation à la Certification de Compétences de DPO
- Des bases de questions d'entrainement pour se préparer à la certification
- Une base documentaire mise à jour de façon continue pour aider les stagiaires dans la pratique quotidienne de leur métier à venir

Modalités d'évaluation et de suivi

- En début et fin de chaque journée, un QCM de 10 questions permet d'évaluer les connaissances acquises pendant la journée de formation.
- Les stagiaires sont aussi évalués sur leur participation aux différents cas pratiques
- Chaque participant signera un document d'émargement permettant de justifier de sa présence, par demi-journée.
    - Pour la formation à distance un document de présence devra être signé et la présence effective sera attestée par le formateur en Visio.
- Il leur sera également demandé de remplir une fiche d'évaluation du contenu de la formation ainsi que du formateur.
- Il lui sera remis enfin une attestation de fin de formation, ainsi qu'un certificat de formation

A la fin de la formation, le formateur évalue les acquis du stagiaire à travers :

- Une note Globale sur /20 permettant de globaliser les acquis de la formation
- Connaissance de la réglementation en matière de protection des données personnelles (note / 20 basée sur les 10 quiz de la formation)
- Compétences dans la réalisation d'audit et conseil en conformité RGPD (note / 20 basée sur la participation aux exercices de groupes)

- Compétences en gestion de projets de conformité (note / 20 basée sur la participation aux exercices de groupes)

Il sera remis au participant un bilan de réalisation reprenant ces 4 critères avec une des mentions suivante pour chaque critère (Acquis, en cours d'acquisition, non acquis, non applicable).

Il sera remis au stagiaire une attestation de suivi un certificat et un bilan de formation.

La formation est sanctionnée par la Validation du BLOC N°2 de la LICENCE Niveau VI "Responsable de la protection des données des Organisations"

Profil du / des Formateur(s)

Nos formateurs ont les compétences suivantes :
- Conseil en protection des données personnelles depuis plus de 3 ans
- Certifiés au Compétences de DPO (selon référentiel CNIL) auprès d'un des organismes agréés par la CNIL
- Formés et agréés pour la formation de DPO par Impact RGPD
- Plus de 5 ans d'expérience en conseil juridique ou en management ou en gestion d'entreprises ou poste de responsabilité équivalente

Informations sur l'accessibilité

Nos sites de formation ainsi que nos modalités pédagogiques ne répondent pas à tous les critères d'accessibilité aux personnes en situation de handicap.

De ce fait, au moment de la phase d'inscription à la formation nous questionnons par oral puis à l'écrit (questionnaire à remplir par le stagiaire) nos stagiaires sur leur besoins spécifiques le cas échéant.

Formation et certification de Compétences de DPO
Contact : 09 52 76 91 76
info@impact-rgpd.fr

Répertoire national

des certifications professionnelles

Responsable de la Protection des Données des Organisations

RNCP N° : 35680

Date de creéation de l'enregistrement :17-06-2021

Date d'échéance de l'enregistrement :17-06-2024

Objectifs et contexte de la certification :

Il y a 50 ans, les technologies de l'information étaient synonymes d'outils d'automatisation. La majorité des projets avaient pour unique objet l'automatisation d'un processus existant afin d'en réduire les coûts. La question du «traitement » est alors à l'avant-scène. Les données ne sont considérées que dans les limites de leurs apports au bon accomplissement des traitements.

Dans le même temps, une nouvelle autorité publique de contrôle voit le jour : la Commission Nationale de l'Informatique et des Libertés (CNIL). En 2004, les pouvoirs de contrôle et de sanction de la CNIL sont renforcés et la fonction de Correspondant Informatique et Libertés (CIL) est créée.

De 2006 à 2016, la gestion des données, ou Data Management, continue à beaucoup évoluer.

Les États membres de l'UE considèrent alors que ces évolutions requièrent un cadre de protection des données plus solide et plus cohérent, assorti d'une application rigoureuse des règles, afin de susciter la confiance qui permettra à l'économie numérique de se développer dans l'ensemble du marché intérieur. C'est dans ce contexte que le « Règlement Général sur la Protection des Données (RGPD) » est adopté. Il entre en application, en France et dans toute l'Europe, le 25 mai 2018.

Avec ce nouveau règlement, le CIL propre à la France disparait et laisse place, au niveau européen, au « Délégué à la Protection des données (DPD) » ou « Data Protection Officer (DPO) ».

La présente certification permet de certifier les compétences de professionnel(e)s directement opérationnel(le)s, capables d'appréhender profondément le RGPD et de guider chaque

département des
organisations vers une
conformité des traitements des données, véritable levier de performance.

Activités visées :

Le Responsable de la Protection des données des Organisations a pour activité principale l'application du respect du cadre légal du traitement classique ou informatique des données. Son intervention qu'elle soit en cours de traitements ou en amont des traitements, commence par un audit des processus afin d'identifier le mode de circulation des données. Cet audit est en réalité réalisé régulièrement afin d'identifier tout risque ou dérive, susceptible de mettre en danger l'Organisation, sur un plan aussi bien informationnel qu'économique.

Il assiste les différents départements pour la mise en œuvre de traitements appropriés des données qu'ils manipulent. Il cartographie, documente, identifie les traitements, afin de s'assurer de l'application du cadre légal et de permettre une mise en conformité en amont des projets. C'est le but ultime de son intervention, que chaque acteur de l'organisation, intègre dans sa pratique un traitement conforme des données notamment à caractère personnel.

Pour cela, le Responsable de la Protection des données des Organisations a un rôle de formateur des départements concernés et de sensibilisateur pour ceux qui ne traitent pas directement ou indirectement de données à caractère personnel.

Il est référent pour l'ensemble du personnel mais aussi pour la Direction Générale.

Compétences attestées :

1. Collaborer avec les différents départements ou services de l'organisation pour identifier les processus organisationnels
2. Répartir les responsabilités des différents acteurs, selon la méthode RACI pour permettre à chacun de s'exprimer et être au clair sur ce qu'il a à faire pour chaque phase.
3. Déterminer un phasage simple et souple prenant en compte les contraintes du projet (Scrum, Kanban, DevOps) et choisir les outils adaptés (Trello, Slack etc.)
4. Partager les objectifs du projet
5. Veiller au respect de la méthode
6. Focusser sur l'aboutissement des actions (méthode scrum)
7. Anticiper les conséquences des décisions prises, pour limiter les risques éventuels
8. Analyser les différents départements, en collaboration avec les directions de chacun d'entre eux, par des entretiens directs ou en cas de télétravail, en distanciel et par l'accès autorisé au système d'information (CRM, comptes rendus d'ateliers collaboratifs…)

9. Référencer les grands traitements de données à caractère personnel
10. Identifier la sécurité des voies d'accès, en tenant compte des situations de télétravail des salariés
11. Identifier la sécurité du système d'information
12. Identifier la sécurité des comportements des collaborateurs et réaliser un focus sur le personnel en télétravail ou dit « nomade »
13. Veiller à la licéité et à la loyauté des traitements des données à caractère personnel en informant et en recueillant le consentement des personnes dont les données sont utilisées, en respectant les obligations légales d responsable du traitement, en appliquant les principes d'interdiction et d'exception dans le traitement des données sensibles etc.
14. Mettre en œuvre le cadre légal des droits des personnes, tel que par exemple le droit d'accès, de rectification ou de refus de profilage
15. Appliquer le principe de minimisation et le principe d'intégrité des données.
16. Choisir pour chaque action, la durée de conservation strictement utile
17. Alerter le responsable du traitement sur son obligation de respecter le RGPD
18. Mettre en place des mesures techniques et organisationnelles appropriées pour que tout projet de l'organisation tienne compte en amont des principes du RGPD (dès la conception)
19. Garantir que seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement soient effectivement traitées (par défaut)
20. Déterminer le fondement juridique du traitement recueillant le consentement clair des personnes concernées, en lien avec une obligation légale, règlementaire, contractuelle, Pour répondre à l'intérêt légitime de l'organisation
21. Décrire les traitements cartographiés en précisant la nature des données personnelles traitées, les finalités des traitements, les durées de conservation (légales ou librement fixées), les éventuels services ou personnes internes ou externes à qui sont transférées ces données et les mesures de sécurisation techniques et organisationnelles des données, y compris en cas de télétravail.
22. Documenter le registre pour les différentes données
23. Permettre la traçabilité par la réalisation de rapports d'audit des processus, de documents reprenant la formulation des recommandations de mise en conformité, destinées aux différentes directions de l'organisation (direction générale, direction de chaque département concerné…), de documents reprenant les actions correctives à réaliser
24. Faciliter la mission des autorités de contrôle et répondre aux diverses demandes de consultations des pièces, documents, registres, justifiant la conformité des traitements des données au RGPD
25. Accompagner la direction générale dans le traitement d'un contrôle de la CNIL ou de toute autorité de contrôle des traitements des données à caractère personnel
26. Signaler une atteinte aux données à caractère personnel traitées par l'organisation par exemple en cas de cyberattaque
27. Dispenser des conseils, sur La méthodologie générale d'application du RGPD au sein de l'organisation

28. Dispenser des conseils sur les impacts de la protection des données et la détermination de la nécessité de mettre en œuvre des analyses d'impacts (AIPD) et d'en vérifier l'exécution, en cas de transferts de données hors Union Européenne, sur les instruments juridiques de transfert susceptibles d'être utilisés
29. Identifier les thématiques à surveiller et investiguer les informations disponibles pour repérer les évolutions légales et la jurisprudence et choisir un outil adapté pour créer une bibliothèque évolutive et accessible
30. Collecter, analyser et traiter l'information
31. Diffuser l'information en créant des documents adaptés et/ou en organisant des événements, en tenant compte dans la mesure du possible, des différentes situations de handicap du personnel utilisateur
32. Utiliser des plateformes collaboratives pour échanger avec les personnels qui travaillent à distance
33. A partir de la politique de communication de l'organisation, en collaboration avec le département communication, choisir les canaux d'information à destination des collaborateurs.
34. Segmenter les informations en fonction des personnels ciblés, en s'appuyant sur les « familles professionnelles » identifiées par le service communication
35. Concevoir des contenus simples, clairs et accessibles pour toutes les fonctions, quel que soit le niveau d'intervention dans l'organigramme et animer un forum interactif, en tenant compte des situations de handicap identifiées au sein de l'organisation
36. Créer des tutoriels, avec l'appui du département communication, en incluant des outils audios ou des sous-titres pour les personnes mal voyantes ou mal entendantes, ou en veillant à utiliser des typographies lisibles
37. Segmenter des événements de sensibilisation au RGPD et à ses conséquences sur les pratiques quotidiennes du personnel et de la Direction Générale

Modalités d'évaluation :

Mise en situation professionnelle, cas problème, QCM, soutenance orale

N° et intitulé du bloc	Liste de compétences	Modalités d'évaluation
RNCP35680BC01 Réalisation et suivi d'un audit	1. Collaborer avec les différents départements ou services de l'organisation	A partir d'un cas problème, le candidat devra cartographier

organisationnel et technique des données à caractère personnel traitées	pour identifier les processus organisationnels 2. Répartir les responsabilités des différents acteurs, selon la méthode RACI 3. Déterminer un phasage simple et souple prenant en compte les contraintes du projet (Scrum, Kanban, DevOps) et choisir les outils adaptés (Trello, Slack etc.) 4. Partager les objectifs du projet 5. Veiller au respect de la méthode 6. Focusser sur l'aboutissement des actions (méthode scrum) 7. Anticiper les conséquences des décisions prises, pour limiter les risques éventuels 8. Analyser les différents départements, en collaboration avec les directions de chacun d'entre eux, par des entretiens directs ou en cas de télétravail, en distanciel et par l'accès autorisé au système d'information (9. Référencer les grands traitements de données à caractère personnel 10. Identifier la sécurité des voies d'accès, en tenant compte des situations de télétravail des salariés 11. Identifier la sécurité du système d'information 12. Analyser les rythmes de mise à jour des logiciels, 13. Mesurer le degré de sécurité des systèmes de sauvegardes, notamment si	des traitements de données et prendre en compte les particularités du système d'information à partir des informations données sur l'organisation, son activité, ses clients et fournisseurs L'évaluation de la mise en situation professionnelle est réalisée par un binôme de jurés professionnels dont une extérieur au centre.

	l'entreprise à recours au cloud ou à tout autre système extérieur (notamment dans le cadre de l'organisation du travail à distance) 14. Identifier la sécurité des comportements des collaborateurs et réaliser un focus sur le personnel en télétravail ou dit « nomade ».	
RNCP35680BC02 Pilotage de la mise en conformité des traitements de données à caractère personnel	1. Veiller à la licéité et à la loyauté des traitements des données à caractère personnel 2. Mettre en œuvre le cadre légal des droits des personnes, tel que par exemple le droit d'accès, de rectification ou de refus de profilage 3. Appliquer le principe de minimisation et le principe d'intégrité des données. 4. Choisir pour chaque action, la durée de conservation strictement utile 5. Alerter le responsable du traitement sur son obligation de respecter le RGPD 6. Mettre en place des mesures techniques et organisationnelles appropriées pour que tout projet de l'organisation tienne compte en amont des principes du RGPD (dès la conception)	Question à Choix Multiples - Contrôle des connaissances juridiques sur la réglementation de la protection des données Mise en situation professionnelle - A partir d'une mise en situation professionnelle réelle ou fictive, réaliser le compte-rendu d'un contrôle de la CNIL portant sur la base d'une plainte individuelle de la violation d'un ou plusieurs droits d'une personne concernée.

	7. Garantir que seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement soient effectivement traitées (par défaut) 8. Déterminer le fondement juridique du traitement 9. Décrire les traitements cartographiés en précisant la nature des données personnelles traitées, les finalités des traitements, les durées de conservation (légales ou librement fixées), les éventuels services ou personnes internes ou externes à qui sont transférées ces données et les mesures de sécurisation techniques et organisationnelles des données, y compris en cas de télétravail. 10. Documenter le registre pour les différentes données 11. Permettre la traçabilité par la réalisation de rapports d'audit des processus, de documents reprenant la formulation des recommandations de mise en conformité, destinées aux différentes directions de l'organisation (direction générale, direction de chaque département concerné…), de documents reprenant les actions correctives à réaliser en identifiant clairement les départements concernés,	Soutenance orale à partir d'une présentation écrite, d'une situation professionnelle vécue au sein de l'organisation d'accueil en alternance ou en stage - Le candidat établit un bilan de la politique de protection des données de l'entreprise dans laquelle il évolue avec les actions de mise en conformité recommandées L'évaluation de la situation professionnelle est réalisée par un binôme de jurés professionnels dont un extérieur au centre.

	les acteurs intervenant dans la réalisation de ces mises en conformité… 12. Faciliter la mission des autorités de contrôle et répondre aux diverses demandes de consultations des pièces, documents, registres, justifiant la conformité des traitements des données au RGPD 13. Accompagner la direction générale dans le traitement d'un contrôle de la CNIL ou de toute autorité de contrôle des traitements des données à caractère personnel 14. Signaler une atteinte aux données à caractère personnel traitées par l'organisation exemple : cyberattaque	
RNCP35680BC03 Conseil, veille et information du personnel et de la direction générale relatifs à la protection des données personnelles	1. Dispenser des conseils, sur la méthodologie générale d'application du RGPD au sein de l'organisation. 2. Dispenser des conseils sur les impacts de la protection des données et la détermination de la nécessité de mettre en œuvre des analyses d'impacts (AIPD) et d'en vérifier l'exécution, en cas de transferts de données hors Union Européenne, sur les instruments juridiques de transfert susceptibles d'être utilisés	Question à Choix Multiples - Contrôle des connaissances sur le processus de veille (10 questions) Mise en situation professionnelle - A partir d'un cas problème, le candidat devra conseiller le responsable du traitement pour résoudre une

	3. Identifier les thématiques à surveiller et investiguer les informations disponibles pour repérer les évolutions légales et la jurisprudence et choisir un outil adapté pour créer une bibliothèque évolutive et accessible 4. Collecter, analyser et traiter l'information 5. Diffuser l'information en créant des documents adaptés et/ou en organisant des événements, en tenant compte dans la mesure du possible, des différentes situations de handicap du personnel utilisateur 6. Utiliser des plateformes collaboratives pour échanger avec les personnels qui travaillent à distance 7. A partir de la politique de communication de l'organisation, en collaboration avec le département communication, choisir les canaux d'information à destination des collaborateurs en tenant compte dans ces choix des différentes situations de handicap pour une accessibilité garantie pour tous 8. Segmenter les informations en fonction des personnels ciblés, en s'appuyant sur les « familles professionnelles »	problématique liée à sa responsabilité. - A partir du contexte du même cas problème, le candidat devra réaliser une analyse d'impact du traitement des données à caractère personnel en amont d'un projet de profilage numérique au sein du département marketing - A partir des données de la politique de communication d'un Groupe fictif, le candidat devra rédiger un communiqué à destination des personnels d'accueil des différentes filiales du Groupe et déterminer les canaux d'information choisis en justifiant ses choix L'évaluation de la situation professionnelle est réalisée par un binôme de jurés

	identifiées par le service communication 9. Concevoir des contenus simples, clairs et accessibles pour toutes les fonctions, quel que soit le niveau d'intervention dans l'organigramme et animer un forum interactif, en tenant compte des situations de handicap identifiées au sein de l'organisation.	professionnels dont un extérieur au centre.
RNCP35680BC04 Sensibilisation et formation des directions métiers et supports et de la Direction Générale à la protection des données personnelles	1. Créer des modules de formation destinés à chaque cible : définir les objectifs et le fil rouge de la formation, définir les méthodes pédagogiques, les activités et les technologies à utiliser, planifier, documenter et faciliter les activités d'apprentissage pour l'apprenant, évaluer les acquis, utiliser les moyens collaboratif et la pédagogie adaptée à des formations à distance, en tenant compte des personnes en situation de handicap 2. Créer des tutoriels, avec l'appui du département communication, en incluant des outils audios ou des sous-titres pour les personnes mal voyantes ou mal entendantes, ou en veillant à utiliser des typographies lisibles	Soutenance orale d'une situation professionnelle vécue au sein de l'organisation d'accueil en alternance ou en stage : - Le candidat relate l'amont et l'aval d'une session de formation sur le RGPD et sur une session de sensibilisation du personnel de son organisation d'accueil L'évaluation de la situation professionnelle est réalisée par un binôme

	3. Segmenter des événements de sensibilisation au RGPD et à ses conséquences sur les pratiques quotidiennes du personnel et de la Direction Générale	de jurés professionnels dont un extérieur au centre

Description des modalités d'acquisition de la certification par capitalisation des blocs de compétences et/ou par équivalence :

La certification est obtenue par cumul de blocs.

SECTEUR D'ACTIVITÉ ET TYPE D'EMPLOI

Secteurs d'activités :

Le Responsable de la Protection des données des Organisations exerce son activité dans des entreprises de différentes tailles et dans les Administrations ou Associations : · PME/PMI · ETI · Grandes entreprises · Administration et collectivités locales · Associations

Le Responsable de la Protection des Données des Organisations exerce en interne, pour plusieurs organisations mutualisées ou en externe au sein d'un cabinet conseil, d'un cabinet d'avocats ou d'ingénierie enfin sous un statut d'indépendant.

Type d'emplois accessibles :

Responsable de la Protection des Données des Organisation

Code(s) ROME :

- K1903 - Défense et conseil juridique
- M1802 - Expertise et support en systèmes d''information

Références juridiques des règlementations d'activité :

Son activité s'inscrit dans le cadre des lois Informatique et Liberté et de la Réglementation Européenne liée à la Protection des Données Personnelles.

Il doit être certifié(e) par un organisme agréé par la CNIL.

Il est obligatoire au
sein des organisations
qui comptent plus de 250 salariés et qui brassent un nombre important de données personnelles (secteur de la santé, de la distribution, du traitement général des données…)

VOIES D'ACCÈS

Le cas échéant, prérequis à la validation des compétences :

Titre ou diplôme de niveau 5 ou de niveau 4 et expérience professionnelle de 5 ans dans le domaine informatique ou juridique.

Validité des composantes acquises :

Voie d'accès à la certification	Oui	Non	Composition des jurys
Après un parcours de formation sous statut d'élève ou d'étudiant	X		Le président du jury est un professionnel extérieur à l'établissement, il est désigné par les membres du Jury. Le Jury est composé de quatre personnes dont 75% de membres extérieurs : · La directrice pédagogique (sans voix délibérative) · Un consultant DPO ayant 5 ans d'expérience · Un N+1 d'un responsable de la protection des données personnels d'une ETI ou Grande entreprise · Un membre d'une association de DPO
Après un parcours de formation continue	X		Le président du jury est un professionnel extérieur à l'établissement, il est désigné par les membres du Jury. Le Jury est composé de quatre personnes dont 75% de membres extérieurs : · La directrice pédagogique (sans voix délibérative)

			· Un(e) consultant(e) DPO ayant 5 ans d'expérience · Un N+1 d'un responsable de la protection des données personnels d'une ETI ou Grande entreprise · Un membre d'une association de DPO
En contrat de professionnalisation	X		Le président du jury est un professionnel extérieur à l'établissement, il est désigné par les membres du Jury. Le Jury est composé de quatre personnes dont 75% de membres extérieurs : · La directrice pédagogique (sans voix délibérative) · Un consultant DPO ayant 5 ans d'expérience · Un N+1 d'un responsable de la protection des données personnels d'une ETI ou Grande entreprise · Un membre d'une association de DPO
Par candidature individuelle		X	-
Par expérience	X		Le Jury est composé de quatre personnes dont 75% de membres extérieurs : · Le responsable du service VAE · Trois professionnels en activité, indépendant de l'organisme de formation
En contrat d'apprentissage	X		Le président du jury est un professionnel extérieur à l'établissement, il est désigné par les membres du Jury. Le Jury est composé de quatre personnes dont 75% de membres extérieurs : · La directrice pédagogique (sans voix délibérative) · Un consultant DPO ayant 5 ans d'expérience

			· Un N+1 d'un responsable de la protection des données personnels d'une ETI ou Grande entreprise · Un membre d'une association de DPO

	Oui	Non
Inscrite au cadre de la Nouvelle Calédonie		X
Inscrite au cadre de la Polynésie française		X

Lien avec d'autres certifications professionnelles, certifications ou habilitations : Non

Organisme(s) préparant à la certification :

Nom légal	Rôle
IMPACT RGPD	Certificateur Habilitation pour former et organiser l'évaluation
SKILLS4ALL	Habilitation pour former et organiser l'évaluation

ORGANIS GESTION LPEP ST REMI	Habilitation pour former et organiser l'évaluation
KEYCE ACADEMY - COLLEGE DE PARIS	Habilitation pour former et organiser l'évaluation

Référentiel d'activité, de compétences et d'évaluation :

Référentiel d'activité, de compétences et d'évaluation