

Délégué à la protection des données (MS)

RNCP38585 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326
Formacode(s)	13238, 31006
Code(s) ROME	K1903, M1806, M1802, M1402, K1601
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	09/02/2024
Date d'échéance	09/02/2027

Certificateur(s)

ASSOCIATION ISEP-EDOUARD BRANLY · SIRET : 78428074500026

Résumé de la certification

OBJECTIFS ET CONTEXTE

Les Délégués à la Protection des Données (DPD) ou Data Protection Officer (DPO) sont les garants de la protection des données personnelles traitées par l'entreprise ou l'administration qui les emploie (responsable de traitement). Ils maîtrisent les enjeux juridiques, économiques et informatiques liés aux traitements de données personnelles.

Ils assurent la relation avec l'autorité de contrôle national : la Commission Nationale de l'Informatique et des Libertés (CNIL).

Ils participent, au sein de la gouvernance globale des données de l'entreprise, à la sécurisation des flux informatiques et veillent au respect des règles édictés par le règlement général à la protection des données personnelles (RGPD).

Ils sensibilisent les acteurs internes (salariés, administrés) et externes (clients, usagers etc.) aux risques et enjeux associés aux données personnelles. Dans le cadre d'une démarche projet, ils définissent avec les différents acteurs les procédures adéquates au respect des principes édictés par le RGPD.

Ils gèrent les risques liés aux violations de données en associant avec toutes les parties prenantes de l'entreprise (Responsable de traitement, Responsable de la sécurité du système d'informations, personnes concernées, etc.).

Les activités du DPO peuvent différer selon qu'il soit externe ou interne à l'entreprise.

En interne, la fonction de DPO peut se cumuler avec un poste déjà existant, par exemple, RSSI, sous réserve de ne pas créer de conflit d'intérêts.

La répartition des activités du DPO dépend des métiers préexistants : ainsi, il peut être amené à travailler davantage sur la sécurité des systèmes d'informations, sur les mentions d'informations, etc. Selon ses activités, le DPO est parfois rattaché à une direction spécifique, même si le rattachement à la direction générale reste le plus fréquent.

Dans le cas où il travaille pour le compte de clients tiers, ce qui est le cas notamment lors d'intervention en tant que prestataires (ESN, cabinet d'avocat), des attentes fortes sont exprimées en matière de capacité d'adaptation et d'intégration dans des contextes divers.

Il peut aussi intervenir en tant que « DPO interne mutualisé » pour le compte de plusieurs organismes, partageant son temps de travail entre ceux-ci. Il peut s'agir par exemple de DPO recrutés par des groupements d'employeurs ou par des groupements de collectivités territoriales, ou des groupements hospitaliers de territoire, tant que ce cumul ne crée pas de conflits d'intérêts. Dans tous les cas, il doit faire directement rapport au niveau le plus élevé de la direction de la structure.

La désignation du DPO est une obligation pour tous les organismes publics et pour les entreprises dont l'activité de base nécessite un traitement de données sensibles (telles que les données de santé) ou un suivi régulier de personnes et à grande échelle. Cette désignation est dès lors un enjeu majeur pour une bonne gouvernance de ces

organismes.

ACTIVITÉS VISÉES

Les activités visées par le titre sont les suivantes :

- Identification des données personnelles, cartographie des flux et traitements associés.
- Identification des données sensibles.
- Détermination des bases légales et finalités de traitements dans le but de les inscrire dans le registre de traitement.
- Identification des acteurs internes et externes associés aux traitements de données personnelles.
- Sensibilisation et formation des acteurs concernés par les traitements de données personnelles par la communication écrite et orale sur des supports adaptés afin de permettre de mobiliser les personnes concernées sur les enjeux associés à l'utilisation des données personnelles.
- Management inclusif et égalitaire de la politique de protection des données personnelles vis-à-vis des acteurs internes et externes
- Identification des traitements à risque.
- Management de la politique de protection des données personnelles du responsable de traitement au sein de la gouvernance et au travers des référents identifiés au sein de l'organisme.
- Actualisation du registre de traitement pour supprimer les traitements obsolètes et intégrer les nouveaux traitements.
- Elaboration et modélisation des outils adaptés pour assurer le respect de la mise en conformité du responsable de traitement.

COMPÉTENCES ATTESTÉES

Dans le cadre du respect du RGPD et des exigences de la CNIL dans la mise en œuvre du métier de DPO, les compétences attestées sont les suivantes :

- Modéliser un schéma de flux de données afin de pouvoir identifier les traitements de données personnelles tout au long du cycle de vie de la donnée dans un domaine et/ou un secteur déterminé (Assurance, Banque, santé, etc.) et permettre ainsi de délimiter le périmètre d'intervention et la responsabilité des acteurs liés à ces traitements de données et du Délégué à la Protection des données personnelles.
- Identifier les fondements (finalités et licéité) liés à la collecte des données personnelles par le responsable de traitement et veiller à leur conformité et leur pertinence (choix de la base légale, choix de la durée de conservation, respect du principe de minimisation, exactitude des données)
- Etudier et identifier les caractéristiques et les enjeux liés à la collecte des données « sensibles » prévues à l'article 9 de la réglementation générale à la protection des données personnelles.
- Identifier les traitements avec transferts de données dans les pays étrangers afin de pouvoir articuler les législations nationales et européennes et les pays tiers ayant une politique de protection de données personnelles adaptée ou non et, le cas échéant, instaurer les mesures juridiques nécessaires (ex : clauses contractuelles types) pour garantir la sécurité de ces transferts.
- Identifier les traitements avec transferts de données vers des sous-traitants et mettre en place le cadre légal de la relation entre le responsable de traitement et le sous-traitant.
- Etablir un registre de traitement conforme à la réglementation pour démontrer la prise en considération par le responsable de traitement des enjeux associés aux données personnelles et répondre ainsi à l'article 30 du règlement général à la protection des données personnelles.
- Modéliser un tableau de bord de suivi de la mise en conformité juridique et s'assurer de son accessibilité pour tous les acteurs internes afin de permettre au responsable de traitement d'avoir une visibilité globale, dans le cadre d'un bilan annuel, des risques et enjeux sur les traitements de données personnelles.
- Communiquer et former dans le cadre d'une démarche inclusive toutes les parties prenantes aux enjeux liés aux traitements de données personnelles (personnel, instances dirigeantes, sous-traitants, etc.) en adaptant son discours en fonction des personnes concernées (ex : situation de handicap) et en s'assurant de l'accès pour toutes les personnes en interne aux documents et mentions relatifs à la gestion et au suivi de la politique de la protection des données.
- Manager une équipe pluridisciplinaire intégrant des personnes en situation de handicap et veiller au respect d'une démarche égalitaire et éthique dans le traitement des données personnelles des acteurs internes et externes.
- Sensibiliser sur les enjeux juridiques et informatiques des traitements intégrant des nouvelles technologies (intelligence artificielle, blockchain etc.) dans le cadre de la démarche préventive prévue par l'article 32 du RGPD et dispenser des conseils sur le suivi et la méthodologie à appliquer dans le cadre d'un traitement à risque.
- Identifier les traitements à risque et veiller sur l'application des mesures de sécurisation organisationnelles et

techniques spécifiques afin de mettre en place au sein du responsable de traitement une politique de prévention des risques fondée sur la disponibilité, l'intégrité et la confidentialité des données.

- Suivre et actualiser les traitements de données personnelles au sein de l'organisme de traitement et assurer une traçabilité des activités effectuées par le responsable de traitement sur ses données personnelles.
- Analyser les impacts sur les traitements existants et mettre en place une politique de protection des données personnelles dès l'origine adaptées aux risques et à la nature des opérations de traitement visant à responsabiliser le responsable de traitement.
- Assurer le respect des durées de conservation des données personnelles initialement prévues lors de la collecte des données en veillant à leur purge, et mettre en place les procédures adaptées pour la gestion des principes et droits prévus pour les personnes concernées (demande de droit d'accès, gestion des mentions d'informations).
- Contrôler le respect par le sous-traitant du cadre légal fixé sur les enjeux de données personnelles
- Superviser l'analyse de risque associé aux traitements à risque, solliciter le cas échéant l'autorisation administrative dans le cas où le traitement a été mis en place malgré un risque résiduel.
- Identifier et prendre les mesures urgentes (notification à l'autorité de contrôle et/ou aux personnes concernées) afin d'assurer la continuité de l'activité du responsable de traitement dans le cadre d'une situation de crise (ex: violation de données).
- Documenter les mesures prises en amont par le responsable de traitement dans le cadre de sa démarche de conformité en intégrant dans un registre particulier les situations critiques (ex : violation de données) afin de démontrer la prise en considération par le responsable de traitement des enjeux en matière de protection des données.
- Savoir préparer et répondre à une demande et/ou un contrôle de l'autorité administrative en vue de pouvoir démontrer sa conformité à la réglementation générale à la protection des données personnelles.

Blocs de compétences

RNCP38585BC01 — Réaliser un audit dans les traitements informatiques et papiers du responsable de traitement dans le but de s'assurer de sa mise en conformité juridique.

LISTE DE COMPÉTENCES

Modéliser un schéma de flux de données afin de pouvoir identifier les traitements de données personnelles tout au long du cycle de vie de la donnée dans un domaine et/ou un secteur déterminé (Assurance, Banque, santé, etc.) et permettre ainsi de délimiter le périmètre d'intervention et la responsabilité des acteurs liés à ces traitements de données et du Délégué à la Protection des données personnelles.

Identifier les fondements (finalités et licéité) liés à la collecte des données personnelles par le responsable de traitement et veiller à leur conformité et leur pertinence (choix de la base légale, choix de la durée de conservation, respect du principe de minimisation, exactitude des données)

Etudier et identifier les caractéristiques et les enjeux liés à la collecte des données « sensibles » prévues à l'article 9 de la réglementation générale à la protection des données personnelles.

Identifier les traitements avec transferts de données dans les pays étrangers afin de pouvoir articuler les législations nationales et européennes et les pays tiers ayant une politique de protection de données personnelles adaptée ou non et, le cas échéant, instaurer les mesures juridiques nécessaires (ex : clauses contractuelles types) pour garantir la sécurité de ces transferts.

Identifier les traitements avec transferts de données vers des sous-traitants et mettre en place le cadre légal de la relation entre le responsable de traitement et le sous-traitant.

Etablir un registre de traitement conforme à la réglementation pour démontrer la prise en considération par le responsable de traitement des enjeux associés aux données personnelles et répondre ainsi à l'article 30 du règlement général à la protection des données personnelles.

MODALITÉS D'ÉVALUATION

Un travail écrit sous forme d'examens et de résolution de cas pratiques permettant de :

- Mesurer les connaissances des principes de base sur la définition de la donnée personnelle, le rôle des différents acteurs, la détermination des bases légales des traitements, les durées de conservation, l'identification des données sensibles, la gestion des sous-traitants, la gestion des traitements avec transferts de données à l'étranger, le registre de traitement.
- Mettre en pratique ces connaissances dans différents domaines (assurance, santé) et secteurs (marketing, ressources humaines).

- Apprécier la bonne application des différentes législations nationales et internationales.

Un projet de groupe, intégrant une évaluation individualisée, est prévue dans le cadre de la définition et la mise en œuvre d'un registre de traitement de données personnelles.

RNCP38585BC02 — Instituer et communiquer une politique de protection de données personnelles dans le but d'impliquer et de mobiliser tous les acteurs concernés par le management et la gestion des traitements de données personnelles.

LISTE DE COMPÉTENCES

Modéliser un tableau de bord de suivi de la mise en conformité juridique et s'assurer de son accessibilité pour tous les acteurs internes afin de permettre au responsable de traitement d'avoir une visibilité globale, dans le cadre d'un bilan annuel, des risques et enjeux sur les traitements de données personnelles.

Communiquer et former dans le cadre d'une démarche inclusive toutes les parties prenantes aux enjeux liés aux traitements de données personnelles (personnel, instances dirigeantes, sous-traitants, etc.) en adaptant son discours en fonction des personnes concernées (ex : situation de handicap) et en s'assurant de l'accès pour toutes les personnes en interne aux documents et mentions relatifs à la gestion et au suivi de la politique de la protection des données.

Manager une équipe pluridisciplinaire intégrant des personnes en situation de handicap et veiller au respect d'une démarche égalitaire et éthique dans le traitement des données personnelles des acteurs internes et externes.

Sensibiliser sur les enjeux juridiques et informatiques des traitements intégrant des nouvelles technologies (intelligence artificielle, blockchain etc.) dans le cadre de la démarche préventive prévue par l'article 32 du RGPD et dispenser des conseils sur le suivi et la méthodologie à appliquer dans le cadre d'un traitement à risque.

Identifier les traitements à risque et veiller sur l'application des mesures de sécurisation organisationnelles et techniques spécifiques afin de mettre en place au sein du responsable de traitement une politique de prévention des risques fondée sur la disponibilité, l'intégrité et la confidentialité des données.

MODALITÉS D'ÉVALUATION

Des projets de groupe, intégrant une évaluation individualisée, prenant en considération les enjeux liés à la gestion opérationnelle (créer des tableaux de bord et des rapports annuels) et au management (gestion d'équipe, formation) des politiques de protection des données personnelles.

Un projet de groupe, intégrant une évaluation individualisée, est prévue dans le cadre de la définition et la mise en œuvre d'une analyse de risque sur un traitement de données personnelles.

Un travail écrit sous forme d'examens et de résolution de cas pratiques sur les enjeux liés à la sécurisation des données personnelles.

RNCP38585BC03 — Piloter la politique de protection des données personnelles pour s'assurer de sa conformité juridique, pouvoir répondre aux autorités administratives et judiciaires et anticiper la gestion et les risques liés aux traitements de données personnelles dans le cadre d'une situation de crise.

LISTE DE COMPÉTENCES

Suivre et actualiser les traitements de données personnelles au sein de l'organisme de traitement et assurer une traçabilité des activités effectuées par le responsable de traitement sur ses données personnelles.

Analyser les impacts sur les traitements existants et mettre en place une politique de protection des données personnelles dès l'origine adaptées aux risques et à la nature des opérations de traitement visant à responsabiliser le responsable de traitement.

Assurer le respect des durées de conservation des données personnelles initialement prévues lors de la collecte des données en veillant à leur purge, et mettre en place les procédures adaptées pour la gestion des principes et droits prévus pour les personnes concernées (demande de droit d'accès, gestion des mentions d'informations).

Contrôler le respect par le sous-traitant du cadre légal fixé sur les enjeux de données personnelles

Superviser l'analyse de risque associé aux traitements à risque, solliciter le cas échéant l'autorisation administrative dans le cas où le traitement a été mis en place malgré un risque résiduel.

Identifier et prendre les mesures urgentes (notification à l'autorité de contrôle et/ou aux personnes concernées) afin d'assurer la continuité de l'activité du responsable de traitement dans le cadre d'une situation de crise (ex: violation de données).

Documenter les mesures prises en amont par le responsable de traitement dans le cadre de sa démarche de conformité en intégrant dans un registre particulier les situations critiques (ex : violation de données) afin de démontrer la prise en considération par le responsable de traitement des enjeux en matière de protection des

données.

Savoir préparer et répondre à une demande et/ou un contrôle de l'autorité administrative en vue de pouvoir démontrer sa conformité à la réglementation générale à la protection des données personnelles.

MODALITÉS D'ÉVALUATION

Un travail écrit sous forme d'examens et de résolution de cas pratiques sur la démarche de conformité envisagée dès l'origine, les durées de conservation, la gestion du cadre contractuel de la relation avec les sous-traitants, la préparation et la gestion d'un contrôle CNIL.

Un projet de groupe, intégrant une évaluation individualisée, est prévue dans le cadre de la définition et la mise en œuvre d'une demande de droit d'accès.

Un projet de groupe, intégrant une évaluation individualisée, est prévue dans le cadre de la définition et la mise en œuvre d'une analyse de risque sur un traitement de données personnelles.

Un travail oral est prévu dans le cadre d'une mise en pratique d'une situation de gestion de crise.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

Le métier de Délégué à la Protection des Données ou Data Protection Officer (DPO) concerne aussi bien le secteur public que privé. L'article 37 du RGPD impose un DPO pour tous les organismes publics et pour les entreprises dont l'activité de base nécessite un traitement de données sensibles (telles que les données de santé) ou un suivi régulier de personnes et à grande échelle.

TYPE D'EMPLOIS ACCESSIBLES

- Délégué à la protection des données personnelles
- Consultant Privacy
- Consultant RGPD
- Juriste protection des données personnelles
- Compliance Officer / Responsable de conformité

RÈGLEMENTATIONS D'ACTIVITÉ

Le métier de DPO est encadré et défini avec précision dans les articles 37 à 39 du RGPD.

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 1 à 5 sur 5.
Facteurs principaux	Manque de main-d'œuvre disponible
Salaire médian (mensuel)	2 854 €
Familles professionnelles (FAP)	L4X80 — Techniciens des services administratifs · tension 4/5 (Élevée) L5X90 — Cadres administratifs, comptables et financiers (hors juristes) · tension 3/5 (Modérée) L5X91 — Juristes et avocats · tension 3/5 (Modérée) M2X93 — Experts et consultants en systèmes d'information · tension 5/5 (Très élevée) U0X91 — Cadres et techniciens de la documentation · tension 1/5 (Très faible)
Projets de recrutement (BMO 2026)	22 541
Jugés difficiles à recruter	35 %
Emplois saisonniers	6 %

Familles professionnelles (FAP)

L4X80 — Techniciens des services administratifs
L5X90 — Cadres administratifs, comptables et financiers (hors juristes)
L5X91 — Juristes et avocats
M2X93 — Experts et consultants en systèmes d'information
U0X91 — Cadres et techniciens de la documentation

Voies d'accès

MODALITÉS D'ACCÈS

Formation initiale, Formation continue, Apprentissage, Contrat de professionnalisation, VAE

PRÉREQUIS À L'ENTRÉE EN FORMATION

L'admission au titre comporte une étude de dossier et un entretien oral.

Sont recevables les candidatures d'étudiants titulaires d'un des diplômes suivants :

- Diplôme d'ingénieur habilité par la Commission des Titres d'Ingénieur (liste CTI)
- Diplôme d'une école de management habilitée à délivrer le grade national de Master (liste CEFDG)
- Diplôme de 3ème cycle habilité par les autorités universitaires (DEA, DESS, Master...) ou diplôme professionnel de niveau BAC + 5
- Diplôme de M1 ou équivalent, pour des personnes justifiant d'au moins trois années d'expérience professionnelle
- Titre inscrit au RNCP niveau 7
- Diplôme étranger équivalent aux diplômes français exigés ci-dessus.

Il existe des conditions d'accès dérogatoires :

- Niveau M1 validé ou équivalent sans expérience professionnelle
- Diplôme de L3 justifiant d'une expérience adaptée de 3 ans minimum
- Candidats justifiant à minima de 5 années d'expérience professionnelle pour lesquelles les activités exercées ont un lien avéré avec les compétences professionnelles visées par la formation. Dans ce cas, ces derniers devront passer par la Validation des acquis personnels et professionnels (VAPP), qui permet d'apprécier les connaissances, les méthodes et les savoir-faire du candidat.

Dans les deux cas ci-dessus, le parcours académique et/ou professionnel devra(ont) démontrer l'acquisition de connaissances et/ou la mise en œuvre de compétences dans domaine de la protection des données personnelles.

COMPOSITION DU JURY — FORMATION INITIALE, FORMATION CONTINUE, APPRENTISSAGE, CONTRAT DE PROFESSIONNALISATION

4 personnes : 2 sont membres de l'ISEP et 2 sont des professionnels du domaine de la protection des données personnelles

COMPOSITION DU JURY — VAE

6 personnes :

- Le Directeur de l'enseignement ou le Directeur de l'Ecole
- 3 Professeurs de l'école
- 2 professionnels de la protection des données personnelles

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	8 987 €
Selon la branche	7 000 € – 9 800 €
Prise en charge	Branches concernées
8 987 €	Valeur par défaut · 184 branches

9 800 €	CNPEFP des sociétés d'assistance, CPNE Casinos, CPNE autoroutes, CPNE de l'ingénierie, des services informatiques et du conseil, CPNE de l'édition de livres, de l'édition phonographique et de l'édition de musique
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
9 000 €	CPNE Banque, CPNE du Commerce de détail et de gros à prédominance alimentaire, CPNEFP de la Mutualité Sociale Agricole
9 276 €	CPNEF de l'Exploitation cinématographique et de la Distribution de films
9 005 €	CPNE FP Branche des magasins du Bricolage
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	09/02/2024
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	09/02/2027
Date de dernière délivrance possible	09/02/2031

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2022	32	1	89 %	93 %
2021	18	0	67 %	78 %

Liens avec d'autres certifications

ANCIENNES VERSIONS

RNCP32106

CORRESPONDANCES (PAR BLOCS)

RNCP32106

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://formation-continue.isep.fr/offres-de-formation/formations-diplomantes/mastere-specialise-management-et-protection-des-donnees-a-caractere-personnel/>

Fiche officielle (France Compétences)

