

Responsable de la Protection des Données des Organisations

RNCP35680 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 6
Code(s) NSF	326, 128g
Formacode(s)	13238, 34085, 31082, 31096
Code(s) ROME	K1903, M1802
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	17/06/2021
Date d'échéance	17/06/2024

Certificateur(s)

ASCENCIA PARIS LA DEFENSE · SIRET : 50123141900034

IMPACT RGPD · SIRET : 84061945600022

IMPACT RGPD · SIRET : 84061945600014

Partenaires habilités

5 organismes habilités, d'après la liste publiée par France compétences : 5 à former et organiser l'évaluation.

Organisme	SIRET	Habilitation
IMPACT RGPD	84061945600022	Former et organiser l'évaluation
JUNIA XP	89085431800015	Former et organiser l'évaluation
KEYCE ACADEMY - COLLEGE DE PARIS	51872913200069	Former et organiser l'évaluation
ORGANIS GESTION LPEP ST REMI	78060980600010	Former et organiser l'évaluation
SKILLS4ALL	82815451800025	Former et organiser l'évaluation

Résumé de la certification

OBJECTIFS ET CONTEXTE

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 disparaît 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

Les activités sont :

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. Focuser 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'un 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, réglementaire, 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 (légal 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 entendant, 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

Blocs de compétences

RNCP35680BC01 — Réalisation et suivi d'un audit organisationnel et technique des données à caractère personnel traitées

LISTE DE COMPÉTENCES

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
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. Focuser 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 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 ».

MODALITÉS D'ÉVALUATION

A partir d'un cas problème, le candidat devra cartographier 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 un extérieur au centre.

RNCP35680BC02 — Pilotage de la mise en conformité des traitements de données à caractère personnel

LISTE DE COMPÉTENCES

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)
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, 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

MODALITÉS D'ÉVALUATION

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.

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.

RNCP35680BC03 — Conseil, veille et information du personnel et de la direction générale relatifs à la protection des données personnelles

LISTE DE COMPÉTENCES

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
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 » 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.

MODALITÉS D'ÉVALUATION

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 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 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

LISTE DE COMPÉTENCES

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 entendant, ou en veillant à utiliser des typographies lisibles
3. 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

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 de jurés professionnels dont un extérieur au centre

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

RÉGLEMENTATIONS 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...)

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

MODALITÉS D'ACCÈS

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

PRÉREQUIS À L'ENTRÉE EN FORMATION

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

COMPOSITION DU JURY — FORMATION INITIALE

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

COMPOSITION DU JURY — FORMATION CONTINUE

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

COMPOSITION DU JURY — APPRENTISSAGE, CONTRAT DE PROFESSIONNALISATION

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

COMPOSITION DU JURY — VAE

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

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	6 932 €
Selon la branche	6 750 € – 7 281 €
Prise en charge	Branches concernées
6 932 €	Valeur par défaut · 209 branches
6 844 €	CPNEFP des commerces et services de l'audiovisuel, de l'électronique et de l'équipement ménager, CPNEFP du Négoce de l'ameublement
7 281 €	CPNE FP Commerce de Détail de l'Horlogerie Bijouterie
6 750 €	CPNE des industries de santé (CPNEIS)

Base légale

Date de décision	17/06/2021
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	17/06/2024

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/35680/>

Se former en apprentissage

Formations en apprentissage	1
Organismes gestionnaires (CFA)	1
Organismes formateurs	1
Régions couvertes	1
Départements couverts	1
Organismes certifiés Qualiopi	1
Sessions	de 09/2025 à 08/2027

Catalogue des formations en apprentissage — réseau des Carif-Oref. Sans frais pour l'alternant : formation financée par l'OPCO de la branche (NPEC).

Entrées et sorties de formation

Entrées en formation	145
Parcours menés à terme	131
Taux d'achèvement	90 %
Période	03/2022 – 10/2024

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

Demande CPF — formations engagées

Dossiers CPF engagés	163
Montant total engagé	348 450 €
Coût moyen par dossier	2 138 €
Durée moyenne	35 h
Période	09/2021 – 06/2024
France compétences	88 %
Reste à charge titulaire	9 %
France Travail	2 %
Entreprise	0 %
État	0 %

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