

Délégué à la protection des données (DPO)

RNCP34776 · RNCP · Publiée

L'essentiel

Niveau de qualification	Niveau 7
Code(s) NSF	326, 128g
Formacode(s)	13254
Code(s) ROME	K1903
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	23/07/2020
Date d'échéance	23/07/2023

Certificateur(s)

ASS FONDATEURS PROTECT INST CATHO LYON · SIRET : 32693006200145

Résumé de la certification

OBJECTIFS ET CONTEXTE

Le métier de DPO (Data Protection Officer ou Délégué à la Protection des Données en français) est né à la suite de la mise en application du RGPD (Règlement Général sur la Protection des Données) à partir du 25 Mai 2018. L'article 37 mentionne les cas dans lesquels les organisations ont l'obligation de désigner un DPO ainsi que les modalités de désignation. Les articles 38 et 39 définissent respectivement les fonctions et missions du DPO. La CNIL (Commission Nationale de l'Informatique et des Libertés) recense les exigences, conditions préalables à remplir et savoir-faire techniques et capacités attendus par le candidat à la certification CNIL.

Ce cadre de référence posé, la profession est en cours de structuration et de définition.

La première étude du Ministère du Travail sur le métier (Printemps 2019) associée aux études terrains montrent que le DPO est un hybride : manager et formateur, il intervient à la fois dans le domaine informatique et dans le domaine juridique. Les professionnels expriment à la fois un besoin de développer des compétences sur tous ces sujets et aussi de les renforcer dans les domaines "gestion de projet et communication".

La certification a en conséquence pour objectif de renforcer les compétences managériales transversales (gestion de projet, gestion d'équipe projet) et les compétences permettant au DPO d'avoir un impact sur la gouvernance, l'appropriation et la diffusion des valeurs éthiques de l'entreprise.

Ainsi les sphères d'expertises du DPO ne se résument pas à celles concernant les aspects techniques et juridiques, mais elles intègrent également les sphères stratégiques et éthiques faisant du DPO un acteur en responsabilité de l'accompagnement au changement.

ACTIVITÉS VISÉES

Le DPO exerce les activités suivantes :

- Piloter la production et la mise en œuvre des politiques et stratégies de la protection des données en collaboration avec l'ensemble des services de l'organisation : le DPO, de manière similaire à celle d'un consultant qualité, identifie les acteurs, données et flux d'information pour co-construire la politique de protection des données et la décliner en axes stratégiques et plans d'actions opérationnels
- Informer, sensibiliser, diffuser une culture "informatique et liberté" des collaborateurs, des acteurs de la protection des données, de la Direction et du responsable de traitement : acteur de l'accompagnement au changement, le DPO organise et réalise toutes les opérations concourant à l'approbation de la politique de protection des données et à la mise en action des collaborateurs sur le sujet
- Analyser, investiguer, auditer et contrôler la conformité des traitements de données : le DPO réalise toutes les opérations nécessaires au contrôle de conformité. Il pilote cette conformité au sein de l'organisation sous forme de

projet transversal, impliquant plusieurs services et les prestataires et fournisseurs externes

- Gérer de manière opérationnelle les risques des traitements de données: le DPO réalise les opérations relatives aux obligations légales en cas d'aléa, en lien avec les autorités de contrôle, les services internes et les propriétaires des données personnelles. Dans un second temps il ajuste les mesures prises en interne pour renforcer la sécurité et participe aux opérations de reconstruction de la réputation de l'entreprise. Pour cette activité, un travail constant de veille juridique et technique sur le sujet de la protection des données doit être réalisé par le DPO. Ce travail, considéré comme une activité à part entière, est garant du bon management de la conformité et de la bonne gestion opérationnelle des risques.

COMPÉTENCES ATTESTÉES

1.Élaborer les politiques et stratégies de protection des données

- Articuler les enjeux juridiques, techniques, économiques, éthiques et la stratégie de protection des données de l'organisation en s'appuyant sur les outils de la qualité pour définir une politique de protection des données
- Analyser le système d'informations en accord avec les ambitions et la stratégie de l'organisation pour déterminer une politique de protection adaptée
- Identifier les rôles et responsabilités des collaborateurs de l'organisation en s'appuyant sur un bilan du système d'informations pour mettre en place les bases du système de gestion de la sécurité des données
- Intégrer les équipes projet en mobilisant les compétences psychologiques et relationnelles pour construire de manière collaborative des politiques et stratégies de protection des données concertées
- Élaborer un cahier des charges des stratégies et actions à mener en s'appuyant sur les normes établies et sur une analyse du système d'informations pour déterminer ses démarches auprès des collaborateurs et dirigeants
- Élaborer des chartes informatiques et des chartes de gouvernance en utilisant un langage simple et compréhensible par tous pour appuyer ses démarches auprès des collaborateurs et dirigeants
- Promouvoir les valeurs éthiques de la protection des données en favorisant leur intégration dans les chartes de gouvernance pour une compliance des données

2.Informer, sensibiliser et former les collaborateurs à la protection des données

- Concevoir une politique de sensibilisation et de formation au sujet de la protection des données en tenant compte des métiers et compétences des collaborateurs et des enjeux de leur rôle au sein de l'organisation pour assurer le bon fonctionnement des procédures
- Concevoir des actions de communication et de formations adaptées aux différents métiers de l'organisation et aux objectifs définis dans la politique de sensibilisation et de formation en s'appuyant sur l'analyse du système d'informations de l'organisation pour assurer le rôle opérationnel des collaborateurs vis-à-vis de la protection des données
- Contrôler l'impact des actions de communication et de formation en les évaluant pour rectifier ou adapter le programme
- Dispenser les programmes de formation et de sensibilisation du personnel et des instances dirigeantes en s'appuyant sur les méthodes pédagogiques adéquates pour assurer une collaboration effective de chacun à la protection des données
- Adapter sa posture, son discours, le choix des modalités pédagogiques en s'ajustant à son public cible (direction, services informatiques, services juridiques, RH, cœur de métier de l'organisation...) et au contexte pour assurer la transmission des messages
- Argumenter son propos en identifiant les réticences et en analysant les freins pour favoriser la coopération
- Synthétiser et adapter un propos technique en identifiant les éléments saillants pour calibrer la forme de son propos en fonction de son public (direction, services informatiques, services juridiques, RH, cœur de métier de l'organisation...)
- Mettre en valeur les actions mises en œuvres et leurs résultats en concevant des rapports écrits à destination du représentant de l'organisation pour informer et responsabiliser le responsable de traitement sur les mesures et risques (bilan annuel)
- Maîtriser ses émotions et ajuster sa posture en s'appuyant sur une connaissance du lien à l'autre pour assurer la prise de parole en public
- Interagir avec l'ensemble des services de l'organisation (juridique, techniques, direction...) en s'appuyant sur une capacité d'adaptation pour faire adhérer l'ensemble des collaborateurs aux processus de protection des données.

3. Assurer la conformité des traitements de données

- Cartographier les traitements de données réalisés dans l'entreprise en s'appuyant sur l'analyse du système d'informations pour établir la documentation de conformité.

- Établir le registre d'activités de traitement et le registre des catégories de traitements en s'appuyant sur l'analyse du système d'informations pour assurer la traçabilité des traitements de données.
- Établir et faire évoluer les processus et procédures de protection des données en collaborant avec l'ensemble des services et s'appuyant sur le cadre légal, les techniques de sécurité et les outils de la qualité afin de prévenir les aléas
- Piloter l'analyse d'impacts en adéquation avec les attendus légaux pour évaluer les risques des traitements de données.
- Déterminer les durées de conservation des données en s'appuyant sur les obligations légales en la matière et les techniques d'archivage pour assurer la compliance des données.
- Piloter des audits de services internes en s'appuyant sur le cadre légal et les indications des autorités de contrôle pour vérifier l'exécution des analyses d'impact et s'assurer de la conformité avec la loi.
- Piloter des audits de conformité de protection des données auprès des fournisseurs et prestataires en s'appuyant sur le cadre légal de la sous-traitance en matière de protection des données pour s'assurer de la conformité des sous-traitants.
- Contrôler la base juridique des traitements de données et le respect des principes de loyauté, transparence, limitation des finalités, minimisation, exactitude, intégrité et confidentialité des traitements de données en s'appuyant sur l'analyse du système d'informations pour assurer la compliance des traitements de données.
- Identifier l'existence d'un transfert de données hors Union européenne en s'appuyant sur le cadre légal de la compliance des données et la compréhension des infrastructures de stockage des données pour déterminer les instruments juridiques et techniques de transfert adéquats.
- Déterminer les précautions à prendre en matière de contenu de zones libres et cookies en s'appuyant sur le cadre légal pour assurer le respect des droits individuels.
- Établir les procédures de réception et de gestion des demandes d'exercices des droits des personnes concernées en s'appuyant sur le cadre légal de la protection des données pour assurer le respect de l'autodétermination des personnes concernées.
- Déterminer les moyens appropriés et le contenu de l'information à fournir en s'appuyant sur la méthode facile à lire et à comprendre et le cadre légal de la protection des données pour assurer le respect de l'autodétermination informationnelle des personnes concernées.

4. Gérer les risques et fuites de données

- Gérer les relations avec les autorités de contrôle en répondant à leur sollicitation afin de faciliter leur action.
- Évaluer les risques encourus et suscités par les activités et processus de l'organisation en tenant compte de la nature, la portée, le contexte et la finalité des traitements de données pour calibrer les plans d'action proposés à la direction de l'organisation.
- Conduire les actions de rectifications des procédures en mobilisant les services concernés et la veille réalisée pour actualiser la conformité et prévenir les fuites de données.
- Mettre en œuvre la gestion des risques en intégrant les groupes projets relatifs aux SI et en appliquant les procédures de gestion de risques afin de prévenir les risques de fuite de données.
- Déterminer la communication nécessaire auprès des autorités de contrôle et des personnes concernées en s'appuyant sur les obligations légales pour assurer l'autodétermination informationnelle des personnes.
- Diriger la cellule de crise en sollicitant les outils de la communication et les valeurs éthiques de l'organisation pour participer à la reconstruction de la réputation de l'organisation.
- Établir la documentation des violations de données en s'appuyant sur les outils des autorités de contrôle pour assurer la traçabilité des fuites de données.
- Conseiller les dirigeants quant aux ajustements des mesures à apporter en s'appuyant sur les évolutions juridiques et technologiques pour prévenir une nouvelle fuite de données.
- Réaliser une veille juridique et technique sur le sujet de la protection des données en consultant de nombreuses sources pour déterminer les actions de rectifications à réaliser.
- Anticiper les évolutions en analysant les informations juridiques et techniques relatives à la protection des données pour mettre en œuvre une réflexion prospective.

Blocs de compétences

RNCP34776BC01 — Elaborer les politiques et stratégies de protection des données

LISTE DE COMPÉTENCES

- C.1.1. Articuler les enjeux juridiques, techniques, économiques, éthiques et la stratégie de protection des données de l'organisation en s'appuyant sur les outils de la qualité pour définir une politique de protection des données
- C.1.2. Analyser le système d'informations en accord avec les ambitions et la stratégie de l'organisation pour déterminer une politique de protection adaptée
- C.1.3. Identifier les rôles et responsabilités des collaborateurs de l'organisation en s'appuyant sur un bilan du système d'informations pour mettre en place les bases du système de gestion de la sécurité des données
- C.1.4. Intégrer les équipes projet en mobilisant les compétences psychologiques et relationnelles pour construire de manière collaborative des politiques et stratégies de protection des données concertées
- C.1.5. Élaborer un cahier des charges des stratégies et actions à mener en s'appuyant sur les normes établies et sur une analyse du système d'informations pour déterminer ses démarches auprès des collaborateurs et dirigeants
- C.1.6. Élaborer des chartes informatiques et des chartes de gouvernance en utilisant un langage simple et compréhensible par tous pour appuyer ses démarches auprès des collaborateurs et dirigeants
- C.1.7. Promouvoir les valeurs éthiques de la protection des données en favorisant leur intégration dans les chartes de gouvernance pour une compliance des données

MODALITÉS D'ÉVALUATION

- Rédaction de notes aux différents services de l'organisation portant sur l'analyse du système d'informations
- Mise en situation professionnelle avec préparation en groupe : proposition écrite d'une charte de gouvernance, d'une politique et d'une stratégie de protection des données remise à un jury composé d'enseignants et de professionnels et présidé par un professionnel.

RNCP34776BC02 — Informer, sensibiliser, former les collaborateurs à la protection des données

LISTE DE COMPÉTENCES

- C2.1. Concevoir une politique de sensibilisation et de formation au sujet de la protection des données en tenant compte des métiers et compétences des collaborateurs et des enjeux de leur rôle au sein de l'organisation pour assurer le bon fonctionnement des procédures
- C2.2. Concevoir des actions de communication et de formations adaptées aux différents métiers de l'organisation et aux objectifs définis dans la politique de sensibilisation et de formation en s'appuyant sur l'analyse du système d'informations de l'organisation pour assurer le rôle opérationnel des collaborateurs vis-à-vis de la protection des données
- C2.3. Contrôler l'impact des actions de communication et de formation en les évaluant pour rectifier ou adapter le programme
- C2.4. Dispenser les programmes de formation et de sensibilisation du personnel et des instances dirigeantes en s'appuyant sur les méthodes pédagogiques adéquates pour assurer une collaboration effective de chacun à la protection des données
- C2.5. Adapter sa posture, son discours, le choix des modalités pédagogiques en s'ajustant à son public cible (direction, services informatiques, services juridiques, RH, cœur de métier de l'organisation...)

- et au contexte pour assurer la transmission des messages
- C.2.6. Argumenter son propos en identifiant les réticences et en analysant les freins pour favoriser la coopération
- C.2.7. Synthétiser et adapter un propos technique en identifiant les éléments saillants pour calibrer la forme de son propos en fonction de son public (direction, services informatiques, services juridiques, RH, cœur de métier de l'organisation...)
- C.2.8. Mettre en valeur les actions mises en œuvres et leurs résultats en concevant des rapports écrits à destination du représentant de l'organisation pour informer et responsabiliser le responsable de traitement sur les mesures et risques (bilan annuel)
- C.2.9. Maîtriser ses émotions et ajuster sa posture en s'appuyant sur une connaissance du lien à l'autre pour assurer la prise de parole en public
- C.2.10. Interagir avec l'ensemble des services de l'organisation (juridique, techniques, direction...) en s'appuyant sur une capacité d'adaptation pour faire adhérer l'ensemble des collaborateurs aux processus de protection des données

MODALITÉS D'ÉVALUATION

- Rédaction de notes à la direction mettant en exergue les enjeux de la protection des données.
- Mise en situation individuelle orale : jeu de rôle, consistant en une action de sensibilisation et de formation auprès des salariés d'une organisation, observé par un jury d'enseignants et de professionnels présidé par un professionnel.

RNCP34776BC03 — Assurer la conformité des traitements de données

LISTE DE COMPÉTENCES

- C.3.1. Cartographier les traitements de données réalisés dans l'entreprise en s'appuyant sur l'analyse du système d'informations pour établir la documentation de conformité.
- C.3.2. Établir le registre d'activités de traitement et le registre des catégories de traitements en s'appuyant sur l'analyse du système d'informations pour assurer la traçabilité des traitements de données
- C.3.3. Établir et faire évoluer les processus et procédures de protection des données en collaborant avec l'ensemble des services et s'appuyant sur le cadre légal, les techniques de sécurité et les outils de la qualité afin de prévenir les aléas
- C.3.4. Piloter l'analyse d'impacts en adéquation avec les attendus légaux pour évaluer les risques des traitements de données
- C.3.5. Déterminer les durées de conservation des données en s'appuyant sur les obligations légales en la matière et les techniques d'archivage pour assurer la compliance des données.
- C.3.6. Piloter des audits de services internes en s'appuyant sur le cadre légal et les indications des autorités de contrôle pour vérifier l'exécution des analyses d'impact et s'assurer de la conformité avec la loi
- C.3.7. Piloter des audits de conformité de protection des données auprès des fournisseurs et prestataires en s'appuyant sur le cadre légal de la sous-traitance en matière de protection des données pour s'assurer de la conformité des sous-traitants.
- C.3.8. Contrôler la base juridique des traitements de données et le respect des principes de loyauté, transparence, limitation des finalités, minimisation, exactitude, intégrité et confidentialité des traitements de données en s'appuyant sur l'analyse du système d'informations pour assurer la compliance des traitements de données
- C.3.9. Identifier l'existence d'un transfert de données hors Union européenne en s'appuyant sur le cadre légal de la compliance des données et

la compréhension des infrastructures de stockage des données pour déterminer les instruments juridiques et techniques de transfert adéquats.

C.3.10. Déterminer les précautions à prendre en matière de contenu de zones libres et cookies en s'appuyant sur le cadre légal pour assurer le respect des droits individuels.

C.3.11. Établir les procédures de réception et de gestion des demandes d'exercices des droits des personnes concernées en s'appuyant sur le cadre légal de la protection des données pour assurer le respect de l'autodétermination des personnes concernées.

C.3.12. Déterminer les moyens appropriés et le contenu de l'information à fournir en s'appuyant sur la méthode facile à lire et à comprendre et le cadre légal de la protection des données pour assurer le respect de l'autodétermination informationnelle des personnes concernées.

MODALITÉS D'ÉVALUATION

- Élaboration de documents de traçabilité de la conformité des traitements, rédaction de clauses liant responsables de traitement et sous-traitant...
- Mise en situation individuelle et écrite : présentation d'un projet de mise en conformité d'une organisation. Le rapport est soumis à un jury composé d'enseignants et de professionnels et présidé par un professionnel.

RNCP34776BC04 — Gérer les risques et fuites de données

LISTE DE COMPÉTENCES

C.4.1. Gérer les relations avec les autorités de contrôle en répondant à leur sollicitation afin de faciliter leur action

C.4.2. Évaluer les risques encourus et suscités par les activités et processus de l'organisation en tenant compte de la nature, la portée, le contexte et la finalité des traitements de données pour calibrer les plans d'action proposés à la direction de l'organisation

C.4.3. Conduire les actions de rectifications des procédures en mobilisant les services concernés et la veille réalisée pour actualiser la conformité et prévenir les fuites de données

C.4.4. Mettre en œuvre la gestion des risques en intégrant les groupes projets relatifs aux SI et en appliquant les procédures de gestion de risques afin de prévenir les risques de fuite de données

C.4.5. Déterminer la communication nécessaire auprès des autorités de contrôle et des personnes concernées en s'appuyant sur les obligations légales pour assurer l'autodétermination informationnelle des personnes.

C.4.6. Diriger la cellule de crise en sollicitant les outils de la communication et les valeurs éthiques de l'organisation pour participer à la reconstruction de la réputation de l'organisation

C.4.7. Établir la documentation des violations de données en s'appuyant sur les outils des autorités de contrôle pour assurer la traçabilité des fuites de données

C.4.8. Conseiller les dirigeants quant aux ajustements des mesures à apporter en s'appuyant sur les évolutions juridiques et technologiques pour prévenir une nouvelle fuite de données

C.4.9. Réaliser une veille juridique et technique sur le sujet de la protection des données en consultant de nombreuses sources pour déterminer les actions de rectifications à réaliser

C.4.10. Anticiper les évolutions en analysant les informations juridiques et techniques relatives à la protection des données pour mettre en œuvre une réflexion prospective

MODALITÉS D'ÉVALUATION

- Rédaction de notes adressées à la direction relatives à la procédure interne en cas de contrôle par la CNIL et aux évolutions nécessaires des processus de protection des données.
- Mise en situation individuelle et orale : présentation d'un plan d'action faisant suite à une fuite de données devant un jury composé d'enseignants et de professionnels et présidé par un professionnel.

Secteur d'activité et type d'emploi

SECTEURS D'ACTIVITÉS

La typologie des employeurs de DPO est multiple. En réalité, elle n'est pas relative à une taille ou un secteur d'activité en particulier.

L'article 37 du RGPD précise les types d'organisations pour lesquels il est nécessaire de recruter un DPO :

- lorsque la gestion des données personnelles exige un suivi régulier et systématique à grande échelle des personnes concernées,

- lorsqu'il s'agit d'un traitement à grande échelle de données dites « sensibles » (données de santé, données biométriques, opinions politiques, convictions religieuses...) et de données à caractère personnel relatives à des condamnations pénales et à des infractions.

TYPE D'EMPLOIS ACCESSIBLES

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

RÉGLEMENTATIONS D'ACTIVITÉ

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

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

Marché du travail

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

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

Voies d'accès

MODALITÉS D'ACCÈS

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

PRÉREQUIS À L'ENTRÉE EN FORMATION

La certification est accessible aux titulaires d'un diplôme de niveau 6, du domaine juridique ou non juridique, acquis par diplôme ou par expérience professionnelle.

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

PROFESSIONNALISATION

Jury composé de 6 membres comprenant 50% de membres de l'UCLy (Directeur Pédagogique de la formation, Responsable d'Études de la formation, Directeur de la Faculté de Droit) et 50% de membres extérieures (professionnels de la protection des données)

Il est présidé par le Directeur de la Faculté de Droit.

COMPOSITION DU JURY — VAE

Jury composé de 6 membres comprenant 50% de membres de l'UCLy (Directeur Pédagogique de la formation, Responsable d'Études de la formation, Directeur de la Faculté de Droit) et 50% de membres extérieures (professionnels de la protection des données)

Il est présidé par l'un des membres extérieurs professionnel de la protection des données. En vertu de l'article R335-8 du Code de l'éducation, la parité hommes / femmes est respectée dans la composition du jury. Les membres du jury de la même organisation que le candidat ou ayant accompagné le candidat dans sa démarche ne participent pas à la délibération.

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	8 668 €
Selon la branche	7 500 € – 8 813 €
Prise en charge	Branches concernées
8 668 €	Valeur par défaut · 209 branches
8 813 €	CPNEFP Mutualité
8 600 €	CPNE de l'édition de livres, de l'édition phonographique et de l'édition de musique
8 280 €	CPNEFP dans les établissements d'enseignement privés sous contrat
7 500 €	CPNE des industries de santé (CPNEIS)

Base légale

Date de décision	23/07/2020
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	23/07/2023

Pour plus d'informations

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rncp/34776/>

Entrées et sorties de formation

Entrées en formation	5
Parcours menés à terme	9
Taux d'achèvement	180 %
Période	07/2022 – 06/2023

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

Demande CPF — formations engagées

Dossiers CPF engagés	11
Montant total engagé	35 920 €
Coût moyen par dossier	3 265 €
Durée moyenne	289 h
Période	10/2020 – 12/2022
France compétences	72 %
Entreprise	13 %
Reste à charge titulaire	13 %
France Travail	3 %

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