

Exercer les fonctions de délégué à la protection des données (DPO)

RS6229 · RS · Publiée

L'essentiel

Code(s) NSF	128g, 326
Formacode(s)	13238, 31006
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	25/01/2023
Date d'échéance	25/01/2025

Certificateur(s)

ECOLE SUP INFORM COMMERCE · SIRET : 45303523000094

Partenaires habilités

4 organismes habilités, d'après la liste publiée par France compétences : 4 à former.

Organisme	SIRET	Habilitation
CERTYOU	80450946100013	Former
INSTITUT SUPERIEUR D'EXCELLENCE STRATEGIQUE ET MANAGERIALE	94858101200010	Former
LEGISCHOOL	98512069000013	Former
QUEST EDUCATION GROUP	83767023100021	Former

Résumé de la certification

OBJECTIFS ET CONTEXTE

Une « donnée personnelle », sur Internet ou sur papier, est « toute information se rapportant à une personne physique identifiée ou identifiable » :

nom, âge, numéro de téléphone, numéro de carte bancaire, sites qui nous intéressent... donnée biométrique, éléments spécifiques propres à notre identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi la voix ou l'image. Ces données doivent être protégées. C'est l'objet du RGPD (Règlement sur la protection des données personnelles), entré en application le 25 mai 2018.

Il s'applique à toute organisation, publique et privée, qui traite des données personnelles (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, utilisation, consultation, communication, et destruction) pour son compte ou non, dès lors qu'elle est établie sur le territoire de l'Union européenne ou que son activité cible directement des résidents européens. Et, il impose des obligations spécifiques à ces organisations pour garantir la protection des données qui leur sont confiées.

Dans ce contexte, le Délégué à la protection des données est chargé de mettre en œuvre la conformité au RGPD au sein de l'organisation qui l'a désigné.

La présente certification s'adresse à toute personne évoluant dans le secteur informatique, juridique, administratif, financier, de la conformité, de l'audit, ..., souhaitant acquérir les compétences qui lui permettront d'endosser le rôle de DPO. Elle répond également au besoin croissant des entreprises d'avoir accès à des professionnels qualifiés pour gérer la protection des données personnelles qu'elles traitent.

COMPÉTENCES ATTESTÉES

Cartographie des traitements de données personnelles

C1 - Recenser les différents traitements de données personnelles en respectant la réglementation, pour les enregistrer dans le registre de traitements des données

C2 - Lister les catégories de données personnelles traitées pour les identifier dans le registre de traitements des données

C3 - Définir les objectifs poursuivis par les opérations de traitements de données en s'appuyant sur la réglementation en vigueur

C4 - Lister les acteurs (internes ou externes) qui traitent ces données, notamment en identifiant clairement les prestataires sous-traitants, afin d'actualiser les clauses de confidentialité

C5 - Recenser les flux en indiquant l'origine et la destination des données, afin notamment d'identifier les éventuels transferts de données hors de l'Union européenne

C6 - Mettre en place le registre de traitements des données personnelles en réponse à l'obligation prévue par le RGPD

Gestion des risques des traitements de données

C7 - Identifier les risques de sécurité et de conformité associés aux opérations de traitement de données, dans un cadre national ou international afin d'en contrôler les impacts

C8 - Évaluer la pertinence d'effectuer une AIPD (analyse d'impact relative à la protection des données) en s'appuyant sur les outils mis à disposition par la CNIL, pour construire un traitement conforme au RGPD et respectueux de la vie privée en cas de détection de traitements de données personnelles susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées

C9 - Mettre en place les mesures de sécurité adaptées pour limiter les risques de violation de données

C10 - Rédiger les procédures de gestion de crise pour prévenir les situations contentieuses, instruire les réclamations, identifier les violations de données et réaliser les signalements à la CNIL

C11 - Rédiger la procédure interne en cas de contrôle de la CNIL (modalités d'accueil, personnes à prévenir, informations à obtenir)

C12 - Identifier et gérer un incident de sécurité et/ou de conformité à la réglementation en matière de protection des données, afin de déterminer la nature de la faille et de mettre en place des solutions de résolution

Mise en place d'un système de management des données personnelles

C13 - Identifier la base juridique sur laquelle se fonde le traitement (par exemple, consentement de la personne, intérêt légitime, contrat, obligation légale) pour déterminer le périmètre réglementaire

C14 - Vérifier que seules les données strictement nécessaires à la poursuite des objectifs sont collectées et traitées pour être en accord avec la réglementation

C15 - Si pertinent, vérifier que les sous-traitants connaissent leurs nouvelles obligations et leurs responsabilités, afin qu'ils puissent également se conformer à la réglementation

C16 - Établir les modalités d'exercice des droits des personnes concernées (droit d'accès, de rectification, droit à la portabilité des données, retrait du consentement...), en respectant le cadre réglementaire, pour recevoir et gérer les demandes d'exercice des droits

C17 - Mettre en place des outils de suivi et de contrôle de l'utilisation des traitements (analyse de logs, détection de données interdites, vérification du respect des durées de conservation, ...), afin d'être alerté en cas de non-respect des procédures de sécurité des données

C18 - Mettre en place un contrôle de l'effectivité des mesures techniques et organisationnelles de protection des données pour identifier les anomalies et dysfonctionnements

C19 - Rédiger la politique générale de traitement des données afin qu'elle soit conforme aux exigences du RGPD, pour informer les personnes concernées par le traitement de leurs données

Communication sur les sujets RGPD

C20 - Communiquer avec la CNIL pour faciliter les échanges en cas de contrôle

- en étant le point de contact de l'organisme sur les sujets RGPD,
- en répondant aux demandes lors d'un contrôle sur place, instruction d'une réclamation, consultation dans le cadre d'une AIPD, notification d'une violation de données, etc

C21 - Communiquer avec les personnes dont les données personnelles sont traitées pour faciliter les échanges en cas de demande d'information ou de réclamation,

- en étant leur point de contact
- en prenant en charge l'organisation du traitement de leurs demandes d'exercice de droits (accès, portabilité, etc.) afin qu'une réponse complète leur soit apportée dans les délais impartis
- et en répondant à toutes leurs questions relatives au traitement de leurs données personnelles

C22 - Communiquer au sein de l'organisme pour sensibiliser la direction et les collaborateurs aux règles régissant la protection des données personnelles :

- en étant l'interlocuteur interne référent pour toute question concernant la protection des données, et si nécessaire au moyen de personnes relais
- en procédant à des actions de communication et de sensibilisation sur le sujet de la protection des données (affiches, guides pratiques, ...)
- en formant en interne, les collaborateurs qui traitent les données au sein de l'organisme sur les grands principes de la protection des données personnelles
- en tenant un tableau de bord des activités menées, afin d'alimenter un point régulier (réunion de direction) ainsi qu'un rapport d'activité régulier à destination de la direction de l'organisme

Mise en place d'un système de veille

C23 – Effectuer une veille permanente (sur la jurisprudence, les publications des autorités de contrôle, ...) pour entretenir ses connaissances techniques et opérationnelles en lien avec les activités de traitement de l'organisme, et à l'occasion de formations et de partages d'expérience avec son réseau de DPO

Voies d'accès

PRÉREQUIS À L'ENTRÉE EN FORMATION

Toute personne évoluant dans le secteur informatique, juridique, administratif, financier, de la conformité, de l'audit, ...

COMPOSITION DU JURY — FORMATION INITIALE, FORMATION CONTINUE

2 professionnels du secteur non intervenant dans l'établissement, dont l'un est président du jury

1 membre de l'organisme certificateur (Directeur ou Responsable pédagogique)

Base légale

Date de décision	25/01/2023
Durée de l'enregistrement	2 ans
Date d'échéance de l'enregistrement	25/01/2025
Date de dernière délivrance possible	25/07/2025

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://esic-online.com/devenir-delegue-a-la-protection-des-donnees-dpo/>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rs/6229/>

Entrées et sorties de formation

Entrées en formation	307
Parcours menés à terme	301
Taux d'achèvement	98 %
Période	02/2023 – 02/2025

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

Demande CPF — formations engagées

Dossiers CPF engagés	333
Montant total engagé	612 573 €

Coût moyen par dossier	1 840 €
Durée moyenne	18 h
Période	02/2023 – 01/2025
France compétences	91 %
Reste à charge titulaire	6 %
France Travail	1 %
Entreprise	1 %
Compte d'engagement citoyen	0 %

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