

Intégrer la compétence juridique dans les missions du Data Protection Officer (DPO)

RS5618 · RS · Publiée

L'essentiel

Code(s) NSF	326p, 128
Formacode(s)	13238, 31006
Type d'enregistrement	Enregistrement sur demande
Date d'enregistrement	24/11/2021
Date d'échéance	24/11/2024

Certificateur(s)

FIDAL FORMATION · SIRET : 34953736500042

Résumé de la certification

OBJECTIFS ET CONTEXTE

Cette certification est destinée aux délégués à la protection des données (ou DPO), qui conseillent et accompagnent les organismes qui les ont désignés, dans leur conformité au RGPD (Règlement Général sur la Protection des Données).

Selon la CNIL (Commission Nationale de l'Informatique et des Libertés), le DPO est au cœur de ce règlement européen, qui constitue le cadre juridique applicable depuis mai 2018 dans toute l'Union européenne. Avant de lui confier cette mission, il est nécessaire de vérifier qu'un DPO dispose des compétences et des moyens nécessaires à l'exercice de ses missions.

L'objectif de cette certification est de contribuer aux compétences du DPO, pour la partie juridique de ses missions. Ainsi, elle lui permet de s'assurer de la mise en conformité de l'organisation pour laquelle il agit, en matière de droit et de pratiques, concernant la protection et la sécurité des données personnelles. Elle est également axée sur la collaboration du DPO avec le responsable de traitement de ces données, pour prévenir les risques juridiques associés aux opérations de traitement, compte tenu de la nature, de la portée, du contexte et des finalités de celles-ci. Elle lui permet en outre de savoir comment coopérer avec les autorités de contrôle concernées.

COMPÉTENCES ATTESTÉES

- C1 : Etablir la cartographie des données personnelles en lien avec la réalité d'une entreprise donnée, afin de pouvoir concrétiser et développer un plan d'actions dynamique de mise en conformité de cette entreprise, avec la réglementation en vigueur.
- C2 : Informer et conseiller les dirigeants d'une structure concernant le déploiement opérationnel, dynamique et sécurisé d'une politique de protection des données, et notamment concernant les cas dans lesquels une analyse d'impact est nécessaire, afin de les aider à la décision dans ce domaine.
- C3 : Déployer, faire appliquer et contrôler une politique de protection des données en s'appuyant sur la prévention des risques juridiques et informatiques et sur la responsabilisation des acteurs, afin de protéger les données d'une violation, la structure d'une intrusion et des dommages potentiels conséquents (anonymisation, chiffrement, pseudonymisation).
- C4 : Concevoir et diffuser des procédures et outils nécessaires au respect des règles applicables au consentement des personnes et à l'exercice de leurs droits, afin de réaliser le traitement de données à caractère personnel dans les règles de l'art, et de répondre aux demandes et plaintes potentielles des consommateurs ou usagers.
- C5 : Tenir le rôle d'interface entre la structure responsable du traitement de données personnelles (par exemple, le Responsable de la Sécurité des Systèmes d'Information RSSI), les instances de contrôle et les personnes concernées, en sachant rendre compte de la conformité des actions mises en place, notamment par la production

d'un registre de traitement des données personnelles approprié au contexte, et a fortiori en prenant des mesures adéquates en cas de gestion de crise.

- C6 : Etablir des contrats avec les différents acteurs de la chaîne de traitement des données à caractère personnel, afin de déterminer le rôle opérationnel et les responsabilités de chacun, et de pouvoir traiter un incident relatif à la protection des données personnelles.
- C7 : Sécuriser le transfert de données dans le cas de traitements internationaux, en appliquant les techniques juridiques adaptées et en tenant compte du droit international, afin d'étendre la conformité RGPD aux activités internationales d'une structure.

Secteur d'activité et type d'emploi

RÈGLEMENTATIONS D'ACTIVITÉ

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.

Voies d'accès

MODALITÉS D'ACCÈS

Formation continue

PRÉREQUIS À L'ENTRÉE EN FORMATION

Bénéficier d'une première expérience en droit, en informatique ou en gestion d'entreprise.

COMPOSITION DU JURY — FORMATION CONTINUE

Les évaluateurs sont des professionnels en charge du sujet RGPD et des avocats formateurs n'étant pas intervenus dans la formation, ayant bénéficié d'une préparation à leur mission d'évaluation.

Ils sont au nombre de 3 et au moins à 66% externes à la structure du certificateur.

Base légale

Date de décision	24/11/2021
Durée de l'enregistrement	3 ans
Date d'échéance de l'enregistrement	24/11/2024

Statistiques

Année	Certifiés	Dont VAE	Insertion 6 mois	Métier 2 ans
2020	22	—	—	—
2019	36	—	—	—

Liens avec d'autres certifications

ANCIENNES VERSIONS

RS3959

Pour plus d'informations

LIEN VERS LE DESCRIPTIF

<https://www.fidalformations.fr/formation/pi15-competences-juridiques-du-data-protection-officer>

Fiche officielle (France Compétences)

<https://www.francecompetences.fr/recherche/rs/5618/>

Entrées et sorties de formation

Entrées en formation	8
Parcours menés à terme	8
Taux d'achèvement	100 %
Période	03/2022 – 02/2025

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

Demande CPF — formations engagées

Dossiers CPF engagés	8
Montant total engagé	22 680 €
Coût moyen par dossier	2 835 €
Durée moyenne	31 h
Période	02/2022 – 09/2024
France compétences	99 %
Reste à charge titulaire	1 %

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