

Les compétences juridiques du Data Protection Officer (DPO)

RS3959 · RS · Publiée

L'essentiel

Code(s) NSF	128
Formacode(s)	13235
Type d'enregistrement	Enregistrement sur demande
Date d'échéance	31/12/2021

Certificateur(s)

FIDAL FORMATION · SIRET : 34953736500042

Résumé de la certification

OBJECTIFS ET CONTEXTE

La certification concerne tous les secteurs et toutes les entreprises au sein desquels des compétences juridiques de DPO sont nécessaires.

Préconiser puis mettre en œuvre les actions nécessaires à la mise en conformité de l'organisation pour laquelle on agit, en matière de droit et de pratiques, nationales et européennes, concernant la protection et la sécurité des données personnelles.

Collaborer avec le responsable de traitement de ces données et tenir compte du risque associé aux opérations de traitement, compte tenu de la nature, de la portée, du contexte et des finalités de celui-ci. Coopérer avec les autorités de contrôle concernées.

COMPÉTENCES ATTESTÉES

- Conduire un projet appliqué à la protection des données personnelles, sans lien hiérarchique, informer et conseiller à ce sujet.
- Mettre en place une prévention et une gestion des risques appliquées à la protection des données personnelles, au moyen d'une cartographie des risques, d'un dispositif d'alertes, de la mise en place de délégations de pouvoir, d'une communication et de formations adaptées.
- Réaliser ou coordonner des audits internes ou externes, appliqués à la protection des données personnelles.
- Mettre en place une politique de conservation des données personnelles (délais et moyens de conservation).
- Déterminer les critères et les moyens de cryptologie de l'entreprise.
- Tenir un registre de traitement des données personnelles et rendre compte au Responsable de traitement ou au sous-traitant.
- Mettre en place l'analyse d'impact d'un traitement concernant la protection des données personnelles et mettre en œuvre un plan d'actions correctives le cas échéant.
- Etablir une politique de sécurité informatique, en collaboration avec les acteurs concernés. Etablir un plan de gestion de crise.
- Créer une politique de gestion des données personnelles afin d'informer les personnes concernées (salariés, clients, consommateurs ...) de leurs droits et des procédures de mise en œuvre de ces droits.
- Formaliser par écrit les relations entre les acteurs traitant les données, leurs rôles et responsabilités.
- Formaliser les flux de transferts transfrontaliers de données personnelles, dans le respect des normes européennes, en tenant compte des conflits de lois, des juridictions et des règles d'ordre public international, le cas échéant.
- Coopérer avec les autorités de contrôle concernées, communiquer les analyses d'impact, consulter la Direction juridique de la CNIL dans le cadre de ses missions.
- Aider à la décision les responsables des activités de e-marketing afin de respecter la réglementation.

- Réaliser une veille permanente sur son domaine d'activité.
- Préparer la conduite d'un projet appliqué à la protection des données dans un contexte d'entreprise donné, et notamment, l'organisation, la planification et la conduite du changement.
- Etablir la cartographie des données personnelles à risque en lien avec la réalité d'une entreprise donnée.
- Appliquer les délais légaux de conservation et de prescription, en tenant compte du contexte des données concernées.
- Déterminer selon les données concernées si celles-ci doivent relever d'une anonymisation ou d'une pseudonymisation.
- Tenir un registre de traitement des données personnelles, approprié à son contexte.
- Préparer les éléments nécessaires à l'analyse d'impact d'un traitement, concernant la protection des données personnelles.
- Etablir une politique de sécurité informatique, en collaboration avec le RSSI (Responsable de Sécurité des Systèmes d'Information).
- Traiter la plainte d'un consommateur, relative au traitement de ses données personnelles.
- Qualifier les responsables de traitement et les sous-traitants.
- Appliquer les outils spécifiques au RGPD (Clauses standard, BCR (Binding Corporate Rules), accords internationaux notamment avec les Etats-Unis), en tenant compte du droit international.
- Traiter un incident relatif à la protection des données personnelles.
- Aider à la décision les responsables des activités de e-marketing afin de respecter la réglementation.

Voies d'accès

MODALITÉS D'ACCÈS

Formation continue, Candidature individuelle

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, CANDIDATURE INDIVIDUELLE

Les évaluateurs sont des avocats formateurs spécialistes de la thématique et ayant bénéficié d'une préparation à leur mission d'évaluation. Ils sont pour 50% au moins externes à la structure du certificateur.

Base légale

Date d'échéance de l'enregistrement 31/12/2021

Liens avec d'autres certifications

NOUVELLE(S) CERTIFICATION(S)

RS6857, RS5618

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/3959/>

Demande CPF — formations engagées

Dossiers CPF engagés	2
Montant total engagé	7 053 €
Coût moyen par dossier	3 527 €

Durée moyenne	21 h
Période	01/2020 – 12/2020
France compétences	100 %

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