Les compétences juridiques du Data Protection Officer (DPO)

CATEGORIE : C

Vue d'ensemble

Domaine(s) d'activité professionnel dans lequel(s) est utilisé la certification :

Transverse : ■ **Tous secteurs**

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

Code(s) NAF : **69.10Z**

Code(s) NSF : **128**

Code(s) ROME : **M1802**, **K1903**

Formacode : **13235**

Date de création de la certification : **05/04/2018**

Mots clés : **données personnelles**, **GDPR**, **RGPD**, **DPO**

Identification

Identifiant : **3959**

Version du : **19/12/2018**

Références

Consensus, reconnaissance ou recommandation :

Formalisé :

- [Règlement \(UE\) 2016/679 du Parlement européen et du Conseil du 27 avril 2016](#)

Non formalisé :

- [Le délégué à la protection des données \(DPO\), CNIL \(Commission Nationale de l'Informatique et des Libertés\)](#)

Descriptif

Objectifs de l'habilitation/certification

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.

Lien avec les certifications professionnelles ou les CQP enregistrés au RNCP

- aucun

Descriptif général des compétences constituant la certification

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).

Public visé par la certification

Tous publics

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.

Modalités générales

4,5 journées de formation préparatoire à la certification (31,5 heures), en discontinu, en présentiel.
Réalisation de nombreux cas pratiques préparatoires à ceux de la certification.
0,5 jour d'évaluations (3,5 heures), en présentiel, à l'issue du parcours.
Le total est de 35 heures.

Liens avec le développement durable

Aucun

Valeur ajoutée pour la mobilité professionnelle et l'emploi

Pour l'individu

Les personnes qui vont être chargées de ce type de mission ou qui souhaitent y prétendre, vont devoir compléter leurs compétences techniques (informatiques, managériales) par les compétences juridiques que leur impose le contexte européen et international en matière de traitement des données personnelles. En ce sens, la certification « Les compétences juridiques du Data Protection Officer » leur apporte la légitimité correspondant à ce besoin.

Pour l'entité utilisatrice

Le Règlement (UE) 2016/679 est applicable depuis le 25 mai 2018, il renforce les obligations des entreprises concernant la protection des données à caractère personnel.
Cette certification permet aux entreprises d'accompagner les salariés concernés et constitue une référence pour les employeurs et les recruteurs, qui y trouveront une visibilité concernant les compétences acquises.

Evaluation / certification

Pré-requis

Centre(s) de passage/certification

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

Compétences évaluées

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.

Niveaux délivrés le cas échéant (hors nomenclature des niveaux de formation de 1969)

Non applicable.

- Ensemble des sites de Fidal Formation (34 sites en métropole et en Martinique) <http://www.fidalformation.fr>

La validité est Permanente

Possibilité de certification partielle : non

Matérialisation officielle de la certification :

Parchemin Fidal Formation, Groupe Fidal

Plus d'informations

Statistiques

Fidal formation a formé plus de 650 personnes sur ce sujet en 2017 et 2018.

Autres sources d'information

<http://www.fidalformation.fr>