DATA PROTECTION OFFICER (H/F)

Description du métier

Obligatoire pour les entreprises disposant de données personnelles à grande échelle, le Data Protection Officer (DPO) est responsable de la sécurisation des données personnelles en entreprise (évolution du rôle d'interlocuteur référent auprès de la Commission Nationale de l'Informatique et des Libertés).

Autres appellations du métier

- Délégué.e à la protection des données, Data Privacy Officer
- Anciennement appelé CIL : Correspondant Informatique et Libertés

Mobilité professionnelle

- Chief Digital Officer
- Juriste d'entreprise

Code ROME

K1903 - Défense et conseil juridique

Accès au métier, formations

- Diplôme d'université science humaines et sociales mention : data protection officier (DPO)
- Master délégué.e à la Protection des données data protection officer
- Master « Management et protection des données à caractère personnel »
- Master « Sécurité de l'information et des systèmes »
- Master Informatique sécurité des systèmes informatiques
- MBA Management de la sécurité des données
- École d'ingénieur en informatique doublé d'une formation juridique
- Master Spécialisé Informatique et libertés
- Master Spécialisé Sécurité de l'informatique et des systèmes
- Master Spécialisé Cybersécurité et cyberdéfense

DATA PROTECTION OFFICER (H/F)

Compétences

RÉALISER UN DIAGNOSTIC DE LA CONFORMITÉ LÉGALE ET RÈGLEMENTAIRE DE L'ORGANISATION SUR LE PLAN "INFORMATIQUE ET LIBERTÉS"

•En collectant toutes les données nécessaires à la définition du contexte, identifier les traitements liés aux données à caractère personnel
•En analysant ces traitements (finalité, consentement, durée de conservation) évaluer la conformité de l'organisation avec le cadre juridique lié à la protection des données soit la loi Informatique et Libertés et le Règlement Européen à la Protection des Données personnelles (RGPD)
•En mettant en relief le niveau de risques afférant à chaque non-conformité, établir un rapport de synthèse présentant le diagnostic de l'existant
•Cartographier les traitements de données personnelles

CONTRÔLER LA MISE EN ŒUVRE D'UNE POLITIQUE DE CONFORMITÉ ET COOPÉRER AVEC L'AUTORITÉ DE CONTRÔLE CNIL

•Gérer les risques au moyen de la réalisation d'une étude d'impact sur la protection des données
•Tenir le registre des traitements
•Etre garant du traitement des demandes des personnes relatives à l'exercice de leurs droits
•Assurer le lien avec la Commission Nationale de l'Informatique et des Libertés (CNIL)
•Mettre en place une veille sur la protection des données
•Disposer d'une expertise relative aux législations nationale et européenne sur la protection des données
•Evaluer les risques et alerter les dirigeants de nouveaux risques

METTRE EN PLACE UNE POLITIQUE PERMETTANT DE VEILLER AU RESPECT DU CADRE LÉGAL "INFORMATIQUE ET LIBERTÉS"

•Rédiger et mettre en place l'ensemble des procédures liées à la règlementation Informatique et Libertés et RGPD
•Organiser la protection des données dès la conception d'un traitement (Privacy By design)
•Animer des sessions de formation des collaborateurs au cadre légal «Informatique et Libertés »
•Afin de réguler les situations conflictuelles gérer les dimensions relationnelles en cherchant des solutions adaptées aux problèmes pouvant se poser tout en respectant les intérêts de chacun