Devenir DPO : Délégué à la protection des données

Durée : 5 jours – 35 heures

Pilote de la mise en œuvre de la conformité RGPD de l'organisation qui l'a désigné, il doit disposer de qualités managériales, de connaissances précises, et de moyens matériels et organisationnels garantis par le responsable de traitement pour lui permettre d'exercer ses missions.

Compétences visées

- Expliquer les grands principes du RGPD : licéité, transparence et loyauté du traitement
- Assurer la conformité au RGPD
- Gérer les équipes métiers pour la sécurité des données
- Sensibiliser les personnes de l'organisation concernée par le RGPD

Objectifs pédagogiques

- Identifier les fonctions stratégiques de l'entreprise concernées par la mise en conformité
- Mettre en œuvre le plan d'actions de conformité au RGPD
- Surveiller la mise en œuvre de la sécurité des données
- Interagir avec la CNIL

Public

DPO, futur DPO, toute personne dont la mission est d'assurer le respect de la protection des données personnelles au sein d'au moins une organisation.

Prérequis

Une compréhension globale du RGPD et des connaissances de base sur les exigences légales actuelles en matière de protection des données est un plus.

Programme

Préambule au RGPD

- Décrire le contexte historique du RGPD
- Rappeler la Loi Informatique et Libertés

Les définitions et mots-clés

- Définir : donnée à caractère personnel, traitement, fichier etc.
- Identifier les concepts du règlement européen : Accountability, Privacy by Design, Privacy by Default, Analyse d'impact…

Les principes du RGPD (et leurs articles)

- Décrire le principe de licéité du traitement : intérêt légitime, consentement explicite
- Décrire le principe de transparence du traitement : limitation des finalités, conservation limitée des données, minimisation, exactitude des données
- Décrire le principe de loyauté du traitement : mise à jour des données et droit à l'oubli, intégrité, confidentialité et responsabilité
- Expliquer la base juridique d'un traitement

La Commission Nationale de l'Informatique et Libertés

- Définir les autorités de contrôle
- Identifier le statut de la CNIL
- Lister les missions de la CNIL
- Décrire les pouvoirs de la CNIL
- Gérer les relations avec la CNIL : répondre à leurs sollicitations et faciliter leur action

Le rôle et les missions du DPO

- Décrire la nomination, la fonction, les responsabilités et les missions du DPO
- Définir le rôle DPO au sein de l'entreprise
- Mise en œuvre d'une politique interne en matière de protection des données à caractère personnel
- Sensibiliser la direction sur les enjeux de la conformité RGPD
- Mettre en place des programmes de formation sur la protection des données en interne
- Identifier le cadre juridique du RGPD
- Lister le contenu du registre d'activités de traitement et du registre des catégories d'activités de traitement
- Identifier la documentation prouvant la conformité au RGPD
- Organiser et participer à des audits internes ou externes
- Assurer la traçabilité de ses activités (outils de suivi, bilan annuel)

Gestion des demandes d'exercice des droits des personnes concernées

- Déterminer les mesures appropriées et le contenu de l'information à fournir aux personnes concernées
- Concevoir des procédures pour recevoir et gérer les demandes d'exercice des droits des personnes concernées

Gestion de la sous-traitance et des transferts hors UE

- Identifier le cadre juridique relatif à la sous-traitance des traitements des données à caractère personnel
- Identifier l'existence de transferts de données hors Union Européenne
- Déterminer les instruments juridiques de transfert susceptibles d'être utilisés

Gestion des risques et l'application de mesures dès la conception et par défaut

- Identifier les méthodologies de l'analyse d'impact relative à la protection des données (AIPD)
- Vérifier l'exécution d'une analyse d'impact (AIPD)
- Mettre en application le « privacy by design » et le « privacy by default »
- Créer un plan de mesures adaptées à la sécurité des données
- Surveiller la mise en œuvre de la sécurité des données

Gestion des incidents

- Identifier la documentation concernant les violations de données
- Faire face à un incident de sécurité
- Mettre en place un plan de continuité de l'activité
- Évaluer l'impact sur la protection des données personnelles et les conséquences
- Concevoir un arbre de décision
- Avertir la CNIL
- Communiquer avec les personnes concernées par la violation de données