

Comment se mettre en conformité avec le RGPD/GDPR

Référence : **SECCONFORM**

Durée : **2 jours**

Certification : **Aucune**

CONNAISSANCES PREALABLES

- Avoir suivi la journée de sensibilisation – (Référence SECGDPR) .
- Avoir suivi la formation DPO (Data Protection Officer - Référence SECDPO) est un plus .

PROFIL DES STAGIAIRES

- Directeurs, responsables et collaborateurs des services juridiques, responsables et collaborateurs des services informatiques, marketing, commerciaux et relations clients, responsables de la sécurité des systèmes d'information, correspondants « Informatique et Libertés », DPO et futurs DPO, chief digital officers, responsables du contrôle interne, des risques, de la conformité, compliance officers.

OBJECTIFS

- Appréhender les nouveaux enjeux en matière de données à caractère personnel instaurés par le RGPD.
- Identifier les actions à mener en interne.
- Maîtriser les éléments clés d'une mise en conformité concrète et adaptée aux nouvelles contraintes et obligations.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Management de la sécurité

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Comprendre le contexte applicable en matière de protection des données à caractère personnel

Les nouveaux défis

Une modification de paradigme

Un accroissement des textes et obligations

Une hausse des sanctions

Une opportunité pour les organismes concernés

Le périmètre

**Périmètre technique : Périmètre économique, Périmètre historique
Périmètre géographique**

Initier une démarche de mise en conformité

Désigner un responsable en charge de la protection des données à caractère personnel

Opportunité ou nécessité de désigner un data protection officer (DPO)

Désignation interne ou externalisation, possibilité de mutualisation, etc.

Qui peut être désigné ? Quelles doivent être ses missions ?

Nouvelle démarche et organisation d'entreprise : vers une gouvernance de la « donnée »

Réaliser un recensement/audit de conformité des traitements

Déterminer le type d'audit approprié en fonction de la maturité et des besoins de l'organisme concerné

Cartographier les traitements

Analyser le niveau de conformité et le niveau de risque associé de chaque traitement au regard des principes essentiels du RGPD

Focus : comment s'assurer du respect du principe de proportionnalité et de minimisation dans les zones de commentaires libres ?

Planifier les actions et chantiers prioritaires

Organiser et documenter ses processus

Comprendre les principes directeurs en matière de protection des données

L'accountability : mettre en place les mesures adéquates, et pouvoir démontrer leur effectivité et leur efficacité

La privacy by design et by default : tenir compte de la protection des données "dès la conception"

Définir et formaliser une politique de gouvernance de la donnée

Organisation interne

Élaboration du (des) registre(s) des traitements : choix de l'outil adéquat, recensement des traitements, actualisation du registre

Focus : élaboration et mise à jour du registre des traitements

Documentation : élaboration d'une politique de protection des données, formalisation des procédures de respect des droits des personnes, conception d'une politique de sécurité des données, mise en place d'une politique d'archivage et de conservation des données

Focus sur l'information des personnes concernées par le traitement

Politique SIF : information, sensibilisation, formation

Organiser et contractualiser les relations entre les différents acteurs