Juridique - Marketing - Informatique

RGPD : mettre l'entreprise en conformité

OBJECTIFS

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

PROGRAMME

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

A. Les nouveaux défis
Une modification de paradigme / Un accroissement des textes et obligations / Une hausse des sanctions / Une opportunité pour les organismes concernés

B. Le périmètre
Périmètre technique : quoi ? / Périmètre économique : pour qui ? / Périmètre historique : quand ? / Périmètre géographique : où ?

II – Initier une démarche de mise en conformité

A. 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 »

B. 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

III – Organiser et documenter ses processus

A. 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»

B. 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

C. Organiser et contractualiser les relations entre les différents acteurs
- Avec les membres du personnel / Avec les sous-traitants / Avec les autres responsables de traitement : l'hypothèse de la coresponsabilité

Exercice pratique : négociation de la clause relative à la protection des données à caractère personnel dans les documents contractuels

Public
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

Pré-requis
Aucun

Options pédagogiques
Alternance de théorie et de pratique

Durée
2 journée (14 heures)

Tarif inter par personne
Adhérent : 910 € HT
Non adhérent : 1450 € HT

La Formatrice :

Laure Landes-Gronowski, *Avocate, experte en droit des technologies de l'information et de la protection des données à caractère personnel. Elle est associée au Pôle IT & Data privacy chez AVISTEM AVOCATS. Elle intervient tant en conseil qu'en contentieux et a à cœur d'accompagner ses clients dans leur transformation digitale afin qu'ils puissent en saisir les opportunités en toute sécurité.*