COMPTABILITE, GESTION, FINANCE

FICHE PROGRAMMATION

AFGES - PROTECTION DES DONNEES PERSONNELLES : QUELLES EXIGENCES POUR SE CONFORMER AU RGPD ?

Public

Auditeur(trice) interne,Collaborateur(trice) en back office secteur bancaire,Comptable - Assistant(e) comptable,Directeur(trice) et responsable d'équipe,Directeur(trice)/Responsable administratif(ve) et financier (e),Responsable et collaborateur(trice) d'un service juridique

Prérequis

Connaissance de l'environnement bancaire et financier

Objectifs pédagogiques

Comprendre les enjeux et les évolutions de la règlementation en matière de protection des données personnelles

Comprendre les exigences du Règlement (UE) 2016/679 du 27 avril 2016 sur la protection des données (« GDPR »)

Prouver sa mise en conformité

Connaître l'étendue des pouvoirs des autorités de protection et leurs moyens de contrôle

Savoir cartographier les risques « Data Protection » et mener des Études d'Impacts sur la Vie Privée (PIA)

Contenu

1- ENVIRONNEMENT ET RÉGLEMENTATION EN MATIÈRE DE PROTECTION DES DONNÉES

Présentation du contexte et des enjeux de la protection des données.

Synthèse des principales composantes du Règlement européen (UE) 2016/679 sur la Protection des données (RGPD/GDPR).

Sources internationales et européenne du droit local.

Rappel des définitions en la matière.

Les risques encourus et leur « saine » gestion.

Présentation de la CNIL en tant qu'autorité de protection nationale.

Étendue et limites des missions des autorités de protection.

2- L'APPLICATION DU RÈGLEMENT AU SEIN DE L'ORGANISATION

Les attentes quant au rôle de Délégué à la Protection des Données (DPO) (fiche de poste).

Les obligations réglementaires :

- Garantir les droits aux personnes concernées.

- Tenue du registre des traitements.

- Analyse d'impacts sur la vie privée (PIA).

- Demandes d'autorisation pour les traitements « sensibles ».

- Maintenir les niveaux de sécurité grâce aux mesures techniques et organisationnelles adéquates.

- Mettre en place le principe de « Privacy by design ».

- Encadrement des transferts internationaux.

La réalisation d'une cartographie des risques "données personnelles" par l'élaboration du registre des traitements et tenant compte de :

- L'identification des risques en lien avec les risques opérations (sécurité des systèmes d'information, cybercriminalité) et risques de non-conformité.

- L'évaluation des risques.

- La gestion et le pilotage des risques.

- Prise en compte dans la cartographie des risques de non-conformité.

- Quelles conséquences sur les PIA (Privacy Impact Analysis) ?

3- LE RÔLE DES ACTEURS

Formation et sensibilisation des collaborateurs.

Gouvernance du dispositif : implication des dirigeants et comitologie.

Le pilotage des différents acteurs : DPO/CIL, contrôles permanents/périodiques, Direction de la conformité, déontologues.

4- LA MISE EN ŒUVRE D'UN DISPOSITIF DE CONTRÔLE

Anticiper et prévenir les contrôles des Autorités de protection.

Les éléments de réponse en cas de contrôles sur pièces.

Comment prouver sa conformité ?

Publicité du rapport, sanctions pénales, jurisprudence.

5- SYNTHÈSE ET CONCLUSION