

RGPD ET PROTECTION DES DONNÉES CLIENT

Objectifs pédagogiques :

- Situer l'architecture des sources applicables : RGPD, loi Informatique et Libertés modifiée, directive ePrivacy et textes sectoriels de l'assurance
- Appliquer les principes de l'article 5 et déterminer la base légale appropriée de l'article 6 pour chaque traitement du cycle assurantiel
- Maîtriser le régime des données sensibles de l'article 9, en particulier les données de santé en souscription et en gestion de sinistre
- Traiter les demandes d'exercice des droits des personnes concernées (articles 12 à 22) dans les délais et les formes requis
- Mettre en œuvre l'accountability : registre (article 30), analyse d'impact (article 35), sécurité (article 32) et notification des violations sous 72 heures (article 33)
- Encadrer la sous-traitance (article 28), positionner le délégué à la protection des données et sécuriser les transferts hors Union européenne (chapitre V)
- Identifier les points de vigilance propres à l'assurance – prospection, télématique, LCB-FT, lutte contre la fraude – et l'incidence des nouveaux textes numériques (AI Act, DORA, Data Act)
- Mesurer l'exposition aux contrôles et aux sanctions de la CNIL et structurer la gouvernance interne de la conformité

Public visé :

Intermédiaires en assurance (IAS), collaborateurs en cabinet, agents généraux, courtiers, conseillers clientèle, conseillers en gestion de patrimoine.

Prérequis :

Aucun. Des connaissances de base en assurance ou en gestion du risque sont un plus.

Durée :

15 heures

Modalité pédagogique :

Formation à distance (e-learning)

Méthodes pédagogiques :

Cours théoriques rédigés, quiz d'évaluation

Attestation :

Attestation de formation délivrée, conforme à l'obligation annuelle de formation continue des IAS

Conformité réglementaire :

Formation conforme à la Directive DDA (UE) 2016/97 et aux articles du Code des assurances relatifs aux IAS

Accessibilité :

Disponible 24h/24 sur tous supports (ordinateur, tablette, smartphone)

PROGRAMME DE FORMATION

Partie I – Architecture juridique, champ d'application et notions clés

Partie II – Principes cardinaux et bases légales du traitement

Partie III – Données sensibles : santé, biométrie, infractions

Partie IV – Droits des personnes concernées

Partie V-A – Accountability : registre, AIPD, sécurité, violations

Partie V-B – Sous-traitance, DPO et transferts internationaux

Partie VI – Points de vigilance assurantiels et nouveaux textes numériques

Partie VII – Contrôle, sanctions, contentieux et gouvernance interne

Conclusion