



Gestion des systèmes d'information

Protection des données

RGPD : gestionnaire de traitements RH

Durée : 0,5 jour

Référence : F05-RGPD-11

Objectifs pédagogiques

Sensibiliser les stagiaires aux impacts du RGPD sur leurs fonctions et leurs missions : périmètre et principes du RGPD ; rôles et responsabilités des parties prenantes (Responsable du Traitement et Sous-Traitant, Responsable Conjoint, Délégué à la Protection des Données, CNIL, autres acteurs) ; enjeux et risques : obligations légales, obligations de résultats ou de moyens, et responsabilités ; cartographie et registre des traitements RH ; obligation de sécurité des données RH ; protection des données RH par défaut et dès la conception ; limitation de la durée de conservation des données RH ; analyses d'impacts ; droits de la personne concernée (information, accès, rectification, effacement, limitation, opposition, consentement et retrait du consentement, recours à la CNIL).

Population concernée

Responsables/gestionnaires opérationnels (ou futurs gestionnaires) de traitements RH ; référents ou correspondants RH (du DPO) ; DPO ; développeurs, chefs de projets et consultants en SIRH.

Connaissances requises

Culture générale de base en matière de droit, d'informatique, et de management de la qualité.

Profil de l'intervenant

Formateur-conseil senior (20 ans d'expérience) titulaire de plusieurs diplômes de niveaux BAC+5 et BAC+8. Compétences de DPO certifiées par l'AFNOR en septembre 2019 (avec l'agrément de la CNIL). 15 ans d'expérience dans le domaine de la protection des données personnelles.

Moyens pédagogiques

Alternance théorie – pratique (cas réels) continue tout au long du stage.
Un support de cours personnalisé par stagiaire.
Un poste informatique formateur avec vidéo projecteur.
Feuille de présence à la demi-journée obligatoire.
Attestation individuelle de formation avec durée (en heures) du stage.

Méthodes d'évaluation

Rappel des objectifs et des prérequis en tour de table.
Contrôle continu par des échanges sur des cas réels tout au long du stage.
Evaluation finale des acquis par le formateur à la demande du client.
Evaluation du stage par chaque stagiaire (questionnaire de satisfaction).



Déroulé pédagogique détaillé page suivante

RAPPELS (si nécessaires)

Parties prenantes : rôles et responsabilités

Définitions réglementaires : Responsable des Traitements, Responsables Conjoint, Sous-Traitants

Place du gestionnaire des traitements RH (ou du référent/correspondant du DPO) dans la gouvernance des DCP

Délégué à la Protection des Données (DPO/DPD) : fonctions, missions (section 4)

Autorité de contrôle nationale (la CNIL) : rôles et pouvoirs

Obligations légales et responsabilités des parties prenantes ; sanctions

Traitements et données à caractère personnel (DCP)

Définitions réglementaires : donnée personnelle, donnée sensible, fichier ou registre, traitement

Périmètre d'application du RGPD

Exemples puisés dans les traitements RH

Enjeux génériques et spécifiques au Responsable des Traitements

TRAITEMENTS RH

Registre des traitements RH

Obligations légales : article 30, preuve et documentation de la conformité

Exemples de fiches registre pour les traitements à finalités RH

Non conformités et risques

Obligations légales : licéité des traitements (article 6) et bases légales des traitements RH

Données RH sensibles et/ou hautement personnelles : NIR, données sociales et/ou médicales, zones libres (recrutement, entretien d'évaluation), condamnations/infractions, appartenance syndicale, rémunérations, contentieux, email/téléphone privé, etc.

Politique de protection des DCP et bonnes pratiques : minimisation des DCP

Limitation de la durée de conservation des DCP (article 5.1.e) et archivage : obligations légales et recommandations de la CNIL pour les traitements RH

Obligation d'information (articles 13 et 14) : mentions d'information pour les traitements RH (contrat de travail, livret d'accueil, notice, etc.)

Recueil du consentement (article 7) : exemples récurrents (droit à l'image, communication des données au CSE, partage de l'information médicale, email/téléphone privé et droit à la vie privée, etc.)

Obligation de sécurité des DCP

Obligations légales : sécurité par défaut, sécurité dès la conception (articles 25 et 32)

Divulgence des données confidentielles à un tiers et secret professionnel

Liens avec le management de la sécurité de l'information (normes ISO 27000 et plus) : confidentialité, intégrité, disponibilité et traçabilité des données.

Chapitres « sécurité des RH » et « acquisition, développement et maintenance des SI(RH) » de la norme ISO 27002

Analyses d'impact

Obligations légales : section 3, traitements RH exemptés par la CNIL

Référentiels CNIL et codes de conduite en matière de traitements RH

Facteurs de risques spécifiques : évaluation/notation/profilage, large échelle, données sensibles

Droits de la personne concernée et notamment du salarié

Obligations légales : chapitre III, articles 7, 13, 14, 15 et plus

Droits de la personne : information, consentement (et retrait du consentement), accès, portabilité, rectification, effacement, limitation, opposition, recours à la CNIL, volontés posthumes, ...

Liens avec les droits des salariés au travail

Liens avec la lutte contre les discriminations et le harcèlement

Problématique du contrôle et de la surveillance des salariés sur leur lieu de travail/pendant leurs horaires de travail : contrôle des horaires, vidéoprotection, géolocalisation, dispositifs biométriques, ...

Consultation des IRP

EN FONCTION DU TEMPS DISPONIBLE

Sous-traitants et tiers

Obligations légales : coresponsabilité avec la sous-traitance (article 28)

Relations contractuelles avec les fournisseurs

Cloud et transferts hors de l'UE (chapitre V)

Notification des violations

Obligations légales : articles 33 et 34

Notification de la CNIL sur son site

Information des personnes concernées