Gestion des systèmes d'information Protection des données RGPD/GDPR et Délégué à la Protection des Données (DPD/DPO)

Durée : 3 à 5 jours

Référence : F05-RGPD-05

Objectifs pédagogiques

S'approprier les connaissances nécessaires à l'accomplissement des missions du DPD/DPO. Maitriser les compétences à mettre en œuvre pour garantir la conformité de l'organisme au regard du RGPD/GDPR et de la Loi Informatique et Libertés. Comprendre son contenu et apprendre à mettre en œuvre le RGPD/GDPR : périmètre, définitions et principes ; rôles et responsabilités des parties prenantes (Responsable du Traitement et Sous-Traitant, Responsable Conjoint, Délégué à la Protection des Données, CNIL) ; enjeux et risques : obligations légales, responsabilités et sanctions ; gouvernance et choix d'un bon pilote ; cartographie et registre des traitements ; documentation et preuve de la conformité ; obligation de sécurité ; limitation de la durée de conservation ; analyse d'impact ; transfert des DCP hors de France ou de l'UE ; droits de la personne concernée ; notification des violations. Promouvoir la diffusion de la « culture » informatique et libertés (protection des données personnelles et de la vie privée).

Population concernée

Futurs DPD/DPO, dirigeants et décideurs responsables de traitements, directeurs des systèmes d'information, responsables informatiques, responsables de la sécurité du système d'information, consultants en systèmes d'information.

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 depuis 2019 sur la base du référentiel de compétences agréé par la CNIL.

Moyens pédagogiques

Alternance théorie - pratique 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

Contrôle continu par des exercices 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

VOLET THEORIQUE

Parties prenantes : rôles et responsabilités

Définitions réglementaires : Responsable des Traitements, Responsable Conjoint, Sous-Traitant

Délégué à la Protection des Données (DPO/DPD) : fonctions, missions, positionnement hiérarchique (section 4) ; caractère obligatoire ou recommandé

Qualifications et compétences du DPO

Indépendance et autorité du DPO : risque de conflit d'intérêt et statut particulier du DPO

Ressources et moyens à mobiliser : DPO interne/externe, DPO à temps plein/partiel

Désignation du DPO à la CNIL ; prise et fin de fonction

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

Comité Européen pour la Protection des Données (CEPD) : rôles et pouvoirs

Obligations légales et responsabilités des parties prenantes ; sanctions ; chaîne répressive de la CNIL

Traitements et registre des traitements

Définitions réglementaires : donnée à caractère personnel (DCP), donnée sensible, fichier ou registre, traitement

Notion de données « hautement personnelles »

Périmètre d'application du RGPD

Obligations légales : article 30

Non conformités et risques

Principes et obligations légales : responsabilité, preuve de la conformité, finalité, licéité (ou base légale) des traitements (article 6), transparence, loyauté, proportionnalité et minimisation des DCP, limitation de la durée de conservation des DCP (article 5.1.e), obligation d'information (articles 13 et 14), recueil du consentement (article 7), respect des droits de la personne (accès, portabilité, rectification, effacement, limitation, opposition), etc.

Non conformités récurrentes : traitement illicite de données personnelles, absence de minimisation et/ou de limitation de la durée de conservation, manquement au droit d'information, consentement non demandé, etc.

Système de management de la protection des données

Obligations légales : preuve et documentation de la conformité

Labels et certifications ; guides de bonne conduite

Principes de la « gestion au plus juste » (minimisation) et de l'amélioration continue (PDCA)

Management de la protection de la vie privée (norme ISO 27701)

Obligation de sécurité des données

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

Normes et obligations pour l'archivage (courant, intermédiaire ou définitif) des DCP

Management de la sécurité de l'information et des systèmes d'information (norme ISO 27000)

Autres domaines du droit concernés

Droit à l'image ; secret des correspondances ; droit d'auteur et droit de propriété intellectuelle ; liberté d'expression, discrimination et diffamation sur Internet ; dispositifs de contrôle/surveillance sur le lieu de travail ; lutte contre le terrorisme et la cybercriminalité ; confiance en l'économie numérique ; etc.

Analyses d'impact

Obligations légales : section 3

Les lignes directrices du CEPD

Quand sont-elles obligatoires ?

Quand ne sont-elles pas obligatoires ?

Sous-traitants et tiers

Obligations légales : coresponsabilité avec la sous-traitance (article 28), communication de DCP à des tiers

Le cas du Responsable Conjoint

Clauses contractuelles : article 28

Cloud et transfert hors de France ou de l'UE (chapitre V)

Droits de la personne concernée

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

Droits de la personne : information, consentement, accès, portabilité, rectification, effacement, limitation, opposition, recours à la CNIL

Notification des violations

Obligations légales : articles 33 et 34

Notification de la CNIL

Information des personnes concernées

VOLET PRATIQUE

Introduction : le délégué à la protection des données

Place du DPO dans la gouvernance des DCP

La notion de gestionnaire opérationnel d'un traitement

Exemples de cas réels

Cartographier les traitements et tenir un registre

Méthodologie et outils d'un audit des traitements

Modèles de registre des traitements

Outils numériques du marché

Exercices et travaux pratiques

Evaluer les non-conformités, les risques et les priorités

Méthodologie du management des risques : norme ISO 31000

Priorisation du risque selon sa vraisemblance et ses conséquences

Homologation du risque résiduel

Méthodologie du management de la sécurité de l'information : norme ISO 27000

Méthodologie d'un audit des non-conformités

Exercices et travaux pratiques

Etablir et suivre un plan d'action

Introduction à la méthodologie de gestion de projet

Classification des exigences par la méthode MoSCoW

Classification des ressources par la méthode RACI

Modèle de plan d'action

Suivi ou pilotage du plan d'action

Management des parties prenantes

Outils numériques du marché

Exercices et travaux pratiques

Documenter un système de management de la protection des données

Méthodologie et principes du management de la qualité : norme ISO 9000

Contenu type d'un SMDCP

Modèles de registres : traitements, violations, demandes des personnes concernées, etc.

Outils numériques du marché

Accompagner les analyses d'impact

Méthodologie d'une pré-étude du risque et d'une analyse d'impact complète en bonne et due forme

Consultation de la CNIL (ou pas)

Suites à donner à l'analyse d'impact

Outils, modèles et ressources proposés par la CNIL

Exercices et travaux pratiques

Gérer les sous-traitants et les tiers

Obtenir les garanties nécessaires

Modèles de conventions/contrats et de clauses contractuelles

Traiter les droits des personnes concernées

Modèles de mentions d'information et de consentement (formulaires, affichettes, contrats, sites web, etc.)

Modèle de politique de protection des DCP

Mettre en place le ou les point(s) d'entrée des demandes des personnes concernées

Processus et délai de traitement des demandes

Modèle de registre des demandes

Exemples de procédures réelles

Outils numériques

Recycler les process existant de gestion des réclamations

Notifier les violations

Service web proposé par la CNIL

Modèle de registre des violations

Exemples de procédures réelles

Recycler les process existant de signalement des anomalies

Renforcer la sécurité

Mesures réglementaires : documentation de la conformité, clauses de confidentialité, mentions légales, codes de conduite, etc.

Mesures organisationnelles : direction, management, collaboration, communication, RH, ventes, archivage, etc.

Mesures techniques : sécurité physique, sécurité logique, cryptage, journaux, sauvegardes, sécurité informatique, etc.

Charte informatique et bon usage des moyens informatiques mis à disposition par l'employeur

Sensibiliser les acteurs concernés

Conduite du changement : changer les mentalités et les habitudes

Prévention et vigilance partagée

Information et sensibilisation

Formation et transfert de compétences

Promotion de la culture de la sécurité (des données personnelles)

Ecoute, compréhension, patience et pédagogie

EXERCICES D'APPLICATION

Mise en œuvre de la méthodologie recommandée

En ateliers pratiques d'au moins 2 heures par traitement servant d'illustrations concrètes : application aux traitements sensibles des stagiaires

EN OPTION

Préparation à la certification des compétences du DPO de l'AFNOR

Conseils du formateur (certifié)