Gestion des systèmes d'information

Sécurité des SI

Mise en œuvre du RGPD/GDPR

Durée : 2 jours

Référence : STD-SI-SSI-2018-6

Objectifs pédagogiques

Comprendre son contenu et apprendre à mettre en œuvre le RGPD/GDPR : périmètre et principes ; rôles et responsabilités des parties prenantes (Responsable du Traitement et Sous-Traitant, 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.

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 (19 ans d'expérience) titulaire de plusieurs diplômes de niveaux BAC+5 et BAC+8.

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

JOUR 1

Parties prenantes : rôles et responsabilités

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

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

Obligations légales et responsabilités des parties prenantes ; sanctions

Traitements et registre des traitements

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

Périmètre d'application du RGPD

Obligations légales : article 30

Non conformités et risques

Obligations légales : licéité des traitements (article 6), 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), 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

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

Obligation de sécurité des DCP

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

Normes pour l'archivage des DCP

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 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

Sous-traitants et tiers

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

Clauses contractuelles

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, opposition

Notification des violations

Obligations légales : articles 33 et 34

Notification de la CNIL

Information des personnes concernées

JOUR 2

Introduction : le délégué à la protection des données

Place du DPO dans la gouvernance des DCP

Cartographier les traitements et tenir un registre

Méthodologie et outils d'un audit des traitements

Modèle 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 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 analyse d'impact (DPIA)

Consultation de la CNIL

Outils 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

Outils numériques

Notifier les violations

Service web proposé par la CNIL

Renforcer la sécurité

Mesures réglementaires : conformité, mentions légales, codes de conduite, etc.

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

Mesures techniques : sécurité physique, sécurité logique, 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