Gestion des systèmes d'information

Sécurité des SI

RGPD/GDPR et Délégué à la Protection des Données (DPD/DPO)

Durée : 2 jours

Référence : STD-SI-SSI-2018-5

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. 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

Expérience (même en tant que simple observateur) du management d'un système d'information ou connaissances théoriques équivalentes.

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

Le RGPD/GDPR 2016/679 et la Loi Informatique et Libertés du 6 janvier 1978 modifiée

Historique ; champ et date d'application ; objectifs ; cadre harmonisé ; principes – concepts – définitions – vocabulaire (donnée personnelle, donnée sensible, traitement, responsable du traitement, sous-traitant, finalité, durée de conservation, consentement, …) ; acteurs concernés ; exigences et obligations ; sanctions et dispositions pénales ; dispositions diverses ; sources.

L'Autorité de Contrôle nationale : la Commission Nationale de l'Informatique et des Libertés

Rôles (missions et fonctions) ; pouvoir ; fonctionnement ; outils et services proposés (notamment en ligne) : lignes directrices pour l'application du RGPD, formulaire de déclaration d'un DPO, formulaire de notification d'une violation, logiciel gratuit d'analyse d'impact (DPIA), modèles de mentions et de clauses, labels, …

Les obligations du Responsable des Traitements/Sous-Traitant et les droits de la personne

Obligation de documentation de fond : études préalables à la mise en œuvre des traitements (cartographie des traitements dans le registre, études de risque, études d'impact sur la vie privé ou DPIA, …) ; sécurité par défaut / dès la conception ; fondement juridique du traitement (licéité) ; limitation de la durée de conservations des données personnelles ; transferts hors de l'Union Européenne ; droit à l'information ; droit d'accès et de rectification ; droit d'opposition et d'effacement (consentement explicite et positif) ; droit à la portabilité ; obligation de notification des violations ; codes de conduite ; management de la sécurité de l'information et des systèmes d'information ; management du risque dans un cadre de sous-traitance ; autres dispositions du RGPD (collaboration entre les autorités nationales, Comité européen de la protection des données, …).

Le Délégué à la Protection des Données personnelles (DPD/DPO)

Rôle et statut ; missions et fonction ; droits et devoirs ; obligation ou recommandation pour le responsable des traitements ; choix du DPO ; qualifications et compétences ; lutte contre le conflit d'intérêt ; protection du DPO dans le cadre de ses missions ; indépendance et subordination vis-à-vis de l'autorité hiérarchique ; positionnement hiérarchique et fonctionnel vis-à-vis des autres acteurs concernés (frontière de sa responsabilité) ; relations avec la CNIL ; traitement des demandes ou DSR (exercice du droit de la personne) ; notification des violations ; DPO à temps plein ou à temps partiel ; DPO interne ou externe ; cas des administrations ; cas des grandes entreprises ; cas des indépendants ; procédure de désignation ; ressources et moyens d'action nécessaires à l'accomplissement de sa mission (charge et méthodologie de travail, outils : registre des traitements, des violations, des DPIA, des DSR, plan d'action, …) ; fin de fonction.

La méthodologie de mise en œuvre du RGPD/GDPR

Désignation d'un pilote (DPO ou non) ; cartographie des traitements ; analyse des écarts avec les obligations légales ; évaluation des risques et des priorités ; homologation du risque résiduel ; élaboration et validation d'un plan d'action ; documentation du plan d'action ; étude(s) d'impact sur la vie privée (DPIA) concernant les traitements majeurs / sensibles ; renforcement de la sécurité des données ; limitation des durées de conservation ; mise à jour des mentions légales et des clauses contractuelles ; collaboration avec les sous-traitants et les éditeurs ; suivi du plan d'action : organisation du processus récurrent de protection des données personnelles (notamment le point d'entrée et la procédure pour l'exercice du droit de la personne ainsi que la notification des violations) ; documentation du processus ; suivi du processus ; communication (information, sensibilisation, formation, promotion de la culture « protection des données », …) ; amélioration continue du processus ; méthodologie de type ISO 27000.

Les liens avec les autres domaines du doit "informatique"

Charte informatique ; directive européenne « E-Privacy » ; sécurité organisationnelle et technique de l'information (norme ISO 27000) ; externalisation vers le Cloud (accord « Privacy Shield », clauses contractuelles types de la Commission Européenne, Cloud « souverain », Code du Patrimoine dans la Fonction publique, …) ; droit à l'image ; droit d'auteur et droits voisins ; limites de la liberté d'expression sur Internet ; dispositifs de contrôles sur le lieu de travail ; lutte contre le terrorisme ; confiance en l'économie numérique ; modernisation de l'Etat (RGS) ; certifications HAS et HDS (établissements de santé) ; etc.