Gestion des systèmes d'information

Protection des données - RGPD

Mise en œuvre des DPIA/AIPD

Durée : 1 jour

Référence : F05-RGPD-8

Objectifs pédagogiques

Comprendre ce qu'est une analyse d'impact sur la protection des données personnelles (AIPD/DPIA) et comment la mettre en œuvre : principes, méthodologies et outils ; obligation de sécurité dès la conception (« *privacy by design* ») ; 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 ; documentation et preuve de la conformité. Application à un traitement sensible par stagiaire.

Population concernée

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

Avoir suivi la formation « Mise en œuvre du RGPD/GDPR » (référence STD-SI-SSI-2018-6) ou connaissances équivalentes acquises par l'expérience.

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.

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

RAPPELS

Analyses d'impact sur la protection des données (AIPD/DPIA)

Obligations légales : section 3

Quand sont-elles obligatoires ?

Quand ne sont-elles pas obligatoires ?

Obligation de sécurité des DCP

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

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) ; qualifications et compétences (selon le référentiel de la CNIL).

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

Obligations légales et responsabilités des parties prenantes ; sanctions

Système de management de la protection des données

Obligations légales : preuve et documentation de la conformité

Principes de l'amélioration continue (PDCA)

METHODOLOGIE : METHODES, TECHNIQUES ET OUTILS

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 et modèles proposés par la CNIL

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

Etablir et suivre un plan d'action (en fonction du temps disponible)

Introduction à la méthodologie de gestion d'un plan d'action / d'une liste de tâches / d'un projet complet

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

EXERCICE D'APPLICATION

Mise en œuvre de la méthodologie recommandée

Un atelier pratique de 3h servant d'illustration concrète : application à un traitement sensible par stagiaire