Kit de survie technique pour DPO

« Pour un DPO, la « naïveté technique » est un réel handicap »

Formation délivrée par Bruno Rasle, délégué général AFCDP, enseignant Mastère Spécialisé ISEP

Formation 2 jours : 14 heures

Objectifs pédagogiques

Au terme de la formation vous serez capable :

- d'interagir avec un informaticien (DSI, RSSI, chef de projet informatique, administrateur de bases de données, webmaster, etc.), de soulever les bonnes questions, de jauger des réponses
- de « décoder » le jargon des informaticiens et de comprendre un ensemble de termes techniques tels que chiffrement, big data, anonymisation, SaaS, Peer to Peer, tokenisation, violation de données, injections SQL, deep learning, cookie, méthode Agile etc.
- de comprendre l'architecture des systèmes d'information et de vous adresser en connaissance de cause aux différents interlocuteurs qui sont impliqués dans leurs spécifications fonctionnelles et leur conception afin de vous assurer du respect du *Privacy by Design*
- de piloter une analyse d'impacts sur les données personnelles, de gérer une notification de violation de données sans être en état de « dépendance » vis-à-vis de vos collègues plus techniques
- de négocier un contrat de sous-traitance avec un prestataire en charge de données collectées par l'entreprise

Pré requis

Connaissances de base Informatique et Liberté
Aucune sur les aspects techniques

Public concerné

Personne destinée à occuper un poste de DPO / DPD

Moyens et méthodes pédagogiques

- Exposé didactique avec participation des apprenants (cas concrets, réponses aux questions,..)
- Apports théoriques (loi, décret, directive, RGPD)
- Nombreux apports documentaires (web, site de la CNIL, décisions de jurisprudences, sanctions, actualités…)
- Nombreux cas concrets et exemples pratiques

Évaluation et sanction de la formation

- Évaluation d'assimilation des connaissances
- Évaluation de satisfaction

PROGRAMME

La formation est constituée de trois parties qui exposent :

- Les principaux composants des systèmes d'information ;
- Les acteurs des technologies de l'information et du numérique (Ecosystème du DPO) ;
- La sécurité des Systèmes d'Information.

Journée : 1

Architecture des Systèmes d'Informations

La compréhension des TIC est faite de manière progressive, en s'appuyant sur des exemples concrets de technologies mises en œuvre lors de traitements de données à caractère personnel (collecte sur un site Web, emailing, traitement au sein d'une base de données, cybersurveillance, constitution d'un *Datalake* pour faire du Big data, anonymisation d'un jeu de données, etc.). En partant des architectures et des techniques, le vocabulaire et les fonctionnalités sont introduits au fur et à mesure afin d'apporter une vue d'ensemble suffisamment précise.

Les architectures (matérielles et logicielles), les technologies, les logiciels, les réseaux, les méthodes, les outils sont décrits avec pragmatisme et sans jargon.

Sont abordés dans cette partie des sujets tels que : les bases de données, le modèle client-serveur, l'architecture trois tiers, les procédures de sauvegarde-restauration, la téléphonie sur IP, la vidéo surveillance, la biométrie, la traçabilité (logs, cookies, réseaux de capteurs, etc.), l'informatique mobile, l'archivage électronique, la virtualisation et le Cloud Computing, etc. Les acronymes n'auront plus de secret pour vous.

L'écosystème du Data Protection Officer

Le Délégué à la protection des données est au front pour contrôler le respect de la loi. Pour espérer être efficace, il doit connaître les métiers des TIC, la gestion et le cycle de vie des projets ainsi que les acteurs qui gravitent autour de leur réalisation.

L'objectif n'est pas de lister tous les acteurs/métiers, ni d'être exhaustif mais de créer/entretenir/développer un réflexe : « En tant que DPO, quelle interaction puis-je avoir avec cette fonction/cette personne ? ». Cette partie prépare également le DPO au rapport aux

autres (contact, relations, frictions, incompréhensions, négociations, collaboration, confiance/défiance, rapports de force, soupçon, etc.).

Les différents interlocuteurs informaticiens avec lesquels un DPO est amené à interagir sont présentés afin de l'aider à travailler et échanger efficacement avec chacun d'eux. Comment discuter avec un RSSI (langage, méthodes, objectifs, outils, etc.), avec un DSI, avec un Risk Manager, avec un chef de projet, un Webmaster, un Scrum master, un urbaniste ? Quelles relations avec les sous-traitants (en mode SaaS, hébergeurs, routeurs d'e-mails, prestataires de tout type) ?

La gestion de projet TIC est présentée afin que le DPO puisse agir de manière appropriée aux phases du projet dans lesquelles il est juste qu'il intervienne et qu'il s'implique.

Journée : 2

Sécurité des Systèmes d'Informations

Parmi les obligations du Responsable de Traitement figure la nécessaire sécurisation des données à caractère personnel qu'il traite. Le Délégué à la protection des données doit donc être en mesure de comprendre les problématiques de sécurité des systèmes d'informations. Nous aborderons également les notions de management de la sécurité et du risque. Les interactions entre le DPO et la DSI concernant la formalisation des analyses de risques (et les études d'impact pour les personnes concernées) sont également couvertes.

Sont abordés dans cette partie des sujets tels que : audit de sécurité, virus, failles de sécurité, correctifs de sécurité/patches, dénis de service, fuite et vol d'informations, sécurité périmétrique, identification et authentification, gestion des droits d'accès, annuaires, signature électronique, spams, failles des réseaux sans fil (Wireless, Wi-Fi, etc.), paiement sécurisé, VPN, technologies dangereuses (le bloc note qui contient des infos cachées), phishing, spoofing, intrusion dans un système, DoS, Cache/proxy, dayzero, exploit, hackers, SoX, PCI, ITIL, ISO 17799 et 27001, etc.

Naturellement, les techniques et dispositifs de protection des données seront également présentées et explicitées ; chiffrement, anonymisation vs pseudonymisation, outils de détection de fuite d'information, ségrégation des rôles, traçabilité, coffre-fort électronique, Forensics, effacement des disques durs, techniques d'intégrité des données, etc.

Cette partie est émaillée de nombreux exemples réels. Des sanctions de la CNIL fondées sur des manquements à la sécurité des traitements illustrent le propos.