FORMATION DE DÉLÉGUÉ À LA PROTECTION DES DONNÉES DANS LES SECTEURS DE LA SÉCURITÉ SOCIALE ET DE LA SANTÉ

Objectif

La formation vous fournit des informations de base (y compris des outils) pour effectuer le travail d'un délégué à la protection des données (DPO) au sein de la sécurité sociale et/ou de la santé. Malgré quelques principes théoriques cette formation sera axée sur la pratique.

Elle est donnée par des experts en sécurité de l'information et en protection des données qui vous expliqueront, à l'aide de divers exemples pratiques, comment ils accomplissent leur travail.
Cette formation tient compte des nouvelles réglementations (NIS, eIDAS, RGPD, …).

A la fin de chaque module, une évaluation sera demandée pour faire les ajustements nécessaires. En ce sens, le contenu d'un module peut être adapté aux commentaires des participants.

Méthodologie

La formation partira des différents éléments du rôle du DPO pour une approche :
- Basée sur l'analyse des risques, les contrôles et les contremesures
- Adapté à l'expérience et au secteur des participants
- Interactive (exercice, discussion, travail, …) pour valider la compréhension des concepts
- Participative pour adapter les cours au public/ animer les exercices

Public cible

Cette formation s'adresse aux DPO's débutants (et adjoints) ou à celles et ceux qui souhaitent améliorer leurs connaissances en lien avec les nouvelles lois et réglementations.

Le contenu de la formation

Jour 1 : Introduction, la gouvernance et la protection des données à caractère personnel

Matin : Introduction & la gouvernance

Cette formation permet de comprendre, d'un côté, la sécurité de l'information dans le cadre de la sécurité sociale et de la santé (lois & règlements de la sécurité de l'information et de la protection des données, les normes minimales) et, de l'autre, la gouvernance en matière de sécurité de l'information (ISMS, les rôles et responsabilités) et le rôle de conseiller en sécurité de l'information;

Après-midi : La protection des données à caractère personnel (RGPD)

En une demi-journée, un rappel des grands thèmes du RGPD et une présentation les moyens pour mettre en pratique les concepts du RGPD seront présentés.

Après cette journée vous serez en mesure d'organiser votre sécurité de l'information, de la documenter, de la gérer et d'assumer le rôle de délégué (ou celui d'adjoint) à la protection des données pour des organisations de tailles moyennes

Jour 2 : La gestion des risques

L'objectif de cette journée est de vous aider à formaliser les risques et de vous informer sur les meilleurs moyens de les traiter au sein de votre organisation.

De manière interactive, la formation portera sur l'ensemble du processus de gestion des risques, y compris la répartition des responsabilités dans le processus, les techniques d'identification des risques et les réponses appropriées aux risques.

La base de la formation consiste d'une part de la norme ISO 31000 pour la gestion des risques des entreprises et d'autre part d'un exercice de sécurité informatique avec lequel vous pouvez appliquer les éléments présentés pendant la journée.

Une attention particulière est également accordée à la gestion des risques dans les projets. Nous vous invitons à vous préparer au travers d'un projet de votre organisation afin que vous puissiez traiter cette partie de manière optimale ; qu'il s'agisse d'un projet informatique, d'un déménagement, du remplacement d'une personne importante, etc…..

Jour 3 : Sécurité technique ICT

Une grande partie de votre rôle en tant que DPO consistera à évaluer les risques, à gérer les technologies de l'information et les données utilisées par votre organisation.
Le but de ce module n'est pas de devenir informaticien ou de coder, mais de comprendre les mécanismes de fonctionnement afin que les bonnes questions soient posées sur les mesures de sécurité.
Bien que certains principes théoriques seront abordés, comme la cryptographie, la sécurité des applications et des réseaux, ... Ce module se concentrera sur des exemples concrets et des listes de contrôle.
La journée se terminera par un petit exercice pour tester vos connaissances dans ce domaine technique.

Jour 4 : La sécurité physique + prise de conscience

Ce module mentionne les différents risques de sécurité physique, les mesures supplémentaires liées à la sécurité de l'information et à la protection des données. Les campagnes de sensibilisation jouent un rôle important à cet égard.

La sécurité physique est la sœur jumelle de la sécurité de l'information. Une clé USB volée ou perdue avec des informations confidentielles peut être un problème majeur. Ou imaginez-vous quelqu'un entre dans votre centre de données sans permission. Vous devez prévoir des mesures de sécurité suffisantes à cet effet.

Le premier maillon faible reste l'homme. Nous devons donc constamment sensibiliser nos collaborateurs à la sécurité "digitale". La journée se terminera par un exercice au cours duquel une campagne de sensibilisation sera élaborée.

Jour 5- La gestion des incidents de sécurité + continuité

Matin : Gestion des incidents de sécurité

Un processus de gestion des incidents fait en sorte qu'il y a moins de panique lorsqu'un incident se produit. Cela vous permet d'apporter une réponse structurée et claire au problème.

Après-midi : Continuité

L'élaboration d'un plan de continuité permet de réagir aux incidents qui mettent en péril la continuité de votre organisation. Ce module expliquera différents aspects du plan de continuité tels que la méthodologie de mise en œuvre d'un ICT-DRP, le cycle de vie des données et les concepts de sauvegarde. Il vous permettra de comprendre les relations entre la continuité d'une organisation et les diverses mesures connexes.

Jour 6 : Privacy & security by design + le Cloud

Matin : Privacy & security by design

Le règlement général sur la protection des données (RGPD) exige que le responsable du traitement prenne des mesures de politique interne par la conception et la normalisation. Ce module décrit les différents concepts qui peuvent vous aider dans leur mise en œuvre et propose des approches pour réaliser ces concepts.

Après-midi : CLOUD

Lors du choix des solutions de gestion de l'information, le cloud est l'une des solutions les plus populaires. Ce module vous aide à comprendre ce qu'est un « cloud » et illustre les différents modèles de « cloud ». Nous illustrons également la meilleure façon d'aborder le choix d'un « cloud » pour répondre aux différents risques de sécurité.

Jour 7 : ***Exercice de synthèse***

Au cours de cette journée, les concepts que vous avez appris dans les différents modules sont mis en pratique à l'aide d'un exemple pratique.

Modalités d'inscription

Le demandeur doit :

- Travailler au sein d'un organisme membre de la Smals
- Être un collaborateur du service de sécurité de l'information dans une institution appartenant au réseau de la sécurité sociale ou de la santé.

Le prix

Le prix de la formation complète est de 1.750 euros.

Annulation & modification

Jusqu'à deux semaines avant le début de la session, la participation peut être annulée.
La Smals se réserve le droit de modifier le programme de formation.
Les inscriptions sont acceptées jusqu'à ce que le nombre maximum de participant soit atteint.