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

Objectif

La formation vous fournira 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. Outre quelques principes théoriques, cette formation sera axée sur la pratique.

Elle sera 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 (législation sur l'IA, la directive NIS 2, le 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
- Adaptée 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 débutants (et adjoints) ou à celles et ceux qui souhaitent améliorer leurs connaissances en lien avec les nouvelles lois et réglementations.

Contenu de la formation

Jour 1 : AM : Introduction au respect de la vie privée, au RGPD et à la sécurité de l'information

Matin : Introduction au RGPD, à la vie privée et à la sécurité de l'information et à la protection des données

Cette formation permet, d'une part, de comprendre la sécurité de l'information et la protection des données dans le cadre de la sécurité sociale et de la santé (lois & réglementations relatives à la sécurité de l'information et à la protection des données, les normes minimales) et, d'autre part, d'apprendre sur la gouvernance en matière de sécurité de l'information (ISMS, les rôles et responsabilités) et le rôle de délégué à la sécurité de l'information et à la protection des données.

Nous prendrons connaissance du RGPD et de quelques principes de base tels que les données à caractère personnel, la confidentialité, l'intégrité, la disponibilité, le traitement, le sous-traitant, le responsable du traitement.

Jour 1 : PM: droits des personnes concernées & responsabilité

Après-midi : droits des personnes concernées et responsabilité

Nous étudierons les droits et obligations des personnes concernées en vertu du RGPD ainsi que les principaux thèmes du RGPD relatifs à la protection du traitement des données à caractère personnel et nous exposerons des outils pour transposer cette réglementation dans la pratique. Nous prendrons connaissance des tâches du DPO et de ses obligations légales. Nous aborderons les droits des personnes concernées et apprendrons comment répondre aux requêtes des citoyens. En outre, nous passerons en revue le Cadre de protection des données et le régime de protection des lanceurs d'alerte.

De cette manière, vous serez en mesure d'organiser, de documenter et de gérer votre sécurité de l'information et d'initier le rôle de délégué à la protection des données et/ou de son suppléant dans les organisations de taille moyenne.

Jour 2 : AM : réglementation dans le cadre de la sécurité de l'information & de la protection de la vie privée

Matin : réglementation dans le cadre de la sécurité de l'information et de la protection de la vie privée

Nous passerons en revue la réglementation nationale et internationale pertinente dans les domaines numérique, financier et de la santé ainsi que leur corrélation. Nous apprendrons à comprendre les principales législations et réglementations belges et européennes qui ont un impact sur la sécurité des données et la cybersécurité. Il s'agit notamment de la loi sur les données, de la législation sur l'IA, DORA, …

Nous prendrons connaissance des principes de base de la directive NIS 2 et des cyberfundamentals et apprendrons à les appliquer au sein d'une organisation. Nous expliquerons en quoi consiste la sécurité de l'information. Ce qui nous amènera à la gestion des risques.

Jour 2 : PM : gestion des risques et mesures de protection (en ce compris DPbyD)

Après-midi : gestion des risques et mesures de protection

L'objectif de cet après-midi sera 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 cette formation aura, d'une part, trait à la norme ISO 31000 pour la gestion des risques des entreprises et, d'autre part, à un exercice de sécurité informatique vous permettant d'appliquer les éléments présentés durant la journée.

Une attention particulière sera également accordée à la gestion des risques dans les projets. Nous vous inviterons à vous préparer au travers d'un projet de votre organisation afin que vous puissiez traiter cette partie de manière optimale. Il pourra s'agir d'un projet informatique, d'un déménagement, du remplacement d'une personne importante, etc.

Jour 3 : AM: fuites de données & gestion des incidents

Matin : fuites de données et gestion des incidents

Nous apprendrons à faire face à des fuites de données et à des incidents et à comprendre le processus de détection, de communication et de suivi de fuites de données. Nous expliquerons aussi comment appliquer la gestion des incidents sur la base de bonnes pratiques. Il sera également précisé comment maintenir le contact avec les autorités de contrôle et comment informer les personnes concernées. Nous vous expliquerons comment établir un plan de réponse aux incidents et vous apprendrez la structure d'un plan de réponse aux incidents.

Jour 3 : PM: Politique, formation et prise de conscience (phishing, sensibilisation, ...)

Après-midi : formation et prise de conscience

Nous apprendrons à développer une politique de sécurité de l'information robuste et à la comprendre, à aider les collaborateurs à prendre conscience des cyber-risques et à les former à reconnaître des menaces. Nous apprendrons aussi à organiser au mieux une campagne de sensibilisation au phishing et aux autres attaques, et à contrer les techniques d'ingénierie sociale.

Jour 4 : AM : sécurité opérationnelle

Matin : sécurité opérationnelle

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 concernant les mesures de sécurité. Nous apprendrons à identifier et à analyser les risques pour les systèmes. Qu'est-ce la protection de la vie privée dès la conception (Security by design) ? Quelles sont les mesures de protection qui existent ? Nous nous intéresserons à la protection du supply chain ainsi que à ses principaux risques du point de vue de la protection de l'information et à ses risques tels que les ransomwares.

Nous apprendrons à comprendre les principes fondamentaux de la protection informatique et à les appliquer.

En plus de préciser certains principes théoriques tels la cryptographie, la gestion des accès, la sécurité des applications et des réseaux, ce module abordera des exemples concrets et des listes de contrôle.

Jour 4 : PM : sécurité physique

Après-midi : sécurité physique

Ce module fait mention des différents risques de sécurité physique et des mesures complémentaires liées à la sécurité de l'information et à la protection des données.

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

Nous apprendrons à comprendre le rôle de la protection physique et nous découvrirons les bonnes pratiques que nous appliquerons pour le contrôle des accès et la surveillance. Quelles sont les menaces physiques qui existent et quelles mesures de sécurité pouvons-nous prendre pour les contrer ?

Jour 5 Incidents de sécurité / Business Continuity

Matin : Gestion des incidents de sécurité

Un processus de gestion des incidents permet de réduire la 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.

Nous apprendrons à évaluer l'impact (au niveau de la confidentialité, de l'intégrité et de la disponibilité) des incidents de sécurité et des cyberattaques sur la continuité. En quoi consiste le business continuity (BCP) et le disaster recovery (DRP) ?

Jour 6 : intelligence artificielle & sécurité de l'information & cybersécurité

Nous apprendrons à comprendre l'impact de la législation relative à l'IA sur l'utilisation des systèmes d'IA dans les organisations. Nous devons apprendre à poser des questions pertinentes. Quels sont les risques de l'IA ? Quelle est la probabilité d'incidents lors de l'utilisation de l'IA ? Comment apprendre à les identifier et à les évaluer ? L'utilisation de l'IA dans le traitement des données présente-t-elle des risques ? Existe-t-il des directives que nous pouvons appliquer pour développer des logiciels d'IA en toute sécurité ? Nous prendrons connaissance des bonnes pratiques de sécurité liées à l'apprentissage automatique et à la chaîne d'approvisionnement logicielle.

Nous prendrons connaissance des bases de l'IA et de la réglementation y afférente afin de déployer l'IA, en toute sécurité et conformément à la législation, dans le cadre du traitement des données à caractère personnel.

Jour 7 : AM : sécurité du Cloud

Matin : sécurité du Cloud

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

Nous prendrons notamment connaissance des différents modèles de cloud, de leurs risques et des principes de protection du cloud computing.

Jour 7 : PM : session libre

Après-midi : session libre

Nous passerons en revue les différents concepts que vous aurez appris dans les différents modules et répondrons à des questions supplémentaires.

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 participants soit atteint.