Formation de délégué à la protection des données dans les secteurs de la sécurité sociale et de la santé

Objectif

La formation propose des informations de base (y compris des outils) pour effectuer le travail de 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.

La formation sera assurée par des experts en sécurité de l'information et en protection des données qui expliqueront, à l'aide de divers exemples pratiques, comment ils effectuent leur travail.
Cette formation tient compte des nouvelles réglementations (RGPD, Règlement sur l'IA, NIS2, ...).

A la fin de chaque module, une évaluation sera demandée afin d'ajuster au besoin la formation. Le contenu d'un module pourra ainsi être adapté suite aux remarques des participants.

Méthodologie

La formation inclut les différents aspects du rôle de DPO. L'approche consistera à :
- fournir des informations sur l'analyse des risques, les contrôles et les contre-mesures;
- se focaliser sur l'expérience et le secteur des participants;
- favoriser l'interaction (exercices, discussion, travail, ...) afin de s'assurer de la compréhension des concepts;
- encourager la participation, ce qui permettra d'adapter la formation au public / animer les exercices.

Groupe-cible
Cette formation s'adresse aux nouveaux DPO (et adjoints) et aux personnes qui souhaitent renforcer leurs connaissances au niveau des nouvelles lois et réglementations.

Contenu de la formation

Jour 1 : AM : Introduction au RGPD et à la sécurité de l'information

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

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

Nous abordons le RGPD et certains concepts 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

Après-midi : Droits des personnes concernées

Nous aborderons les droits et obligations des personnes concernées conformément au RGPD ainsi que les principaux thèmes du RGPD en ce qui concerne la protection du traitement des données à caractère personnel et nous présenterons des outils permettant d'appliquer cette réglementation dans la pratique. Nous prendrons connaissance des tâches du DPO et de ses obligations légales. Nous examinerons les droits des personnes concernées et la manière de traiter les demandes des citoyens. Nous aborderons également le « cadre de protection des données » et le règlement relatif aux lanceurs d'alerte.

Ceci doit permettre d'organiser, de documenter et de gérer la sécurité de l'information et d'assurer le rôle de délégué à la protection des données et/ou de son suppléant au sein d'organisations de taille moyenne.

Jour 2 : AM : Réglementation relative à la sécurité de l'information et à la protection des données

Matin : Réglementation relative à la sécurité de l'information et à la protection des données

Nous donnerons un aperçu de la réglementation pertinente au niveau national et international dans les domaines numériques, financiers et de la santé et leur corrélation. Nous prendrons connaissance des principales législations et réglementations belges et européennes qui portent sur la sécurité des données et la cybersécurité. Il s'agit notamment du Règlement sur les données, du Règlement sur l'IA, DORA, ...

Nous aborderons les principes de base du NIS 2 et les CyberFundamentals et nous 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 cette session est d'aider à formaliser les risques et d'informer sur les meilleures façons de les traiter au sein de l'organisation.

La formation portera de manière interactive 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 sera, d'une part, la norme ISO 31000 pour la gestion des risques dans les entreprises et, d'autre part, un exercice de sécurité de l'information permettant d'appliquer les éléments présentés durant la journée.

Une attention particulière sera également accordée à la gestion des risques dans le cadre de projets. Nous invitons les participants à préparer un projet de l'organisation afin que cet aspect soit intégré de manière optimale ; il peut s'agir d'un projet IT, d'un déménagement, du remplacement d'une personne importante, etc.

Jour 3 : AM : Incidents et fuites de données

Matin : La gestion des incidents de sécurité et des fuites de données

Dans un monde où la numérisation prend une place de plus en plus prépondérante, les organisations deviennent de plus en plus dépendantes de leur système IT. En même temps, la quantité de données sensibles stockées dans ces systèmes augmente de manière exponentielle. Ceci rend les organisations vulnérables aux incidents de cybersécurité et aux fuites de données.

Au cours de cette journée, nous aborderons le contexte des incidents de cybersécurité, les implications juridiques, la cause des incidents et expliquerons comment réagir de manière efficace grâce à des processus de détection et de réponse aux incidents.

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

Après-midi : Formation et sensibilisation

Nous apprendrons à développer et appréhender une politique de sécurité de l'information robuste. Comment faire en sorte que les collaborateurs soient conscients des risques de cybersécurité et comment leur apprendre à reconnaître les menaces ? Comment organiser une campagne de sensibilisation concernant le phishing et d'autres types d'attaques et comment déjouer les techniques d'ingénierie sociale. Nous aborderons aussi plus en détail les conséquences de ransomware. Quelles sont les techniques utilisées par les agresseurs et comment se protéger ?

Jour 4 : AM : Sécurité opérationnelle

Matin : sécurité opérationnelle

Une grande partie du rôle de DPO consiste à évaluer les risques, à gérer les technologies de l'information et les données utilisées par l'organisation.

Le but de ce module n'est pas de former des informaticiens ou d'apprendre à coder, mais de bien comprendre les modes de fonctionnement de sorte à poser les questions adéquates en ce qui concerne les mesures de sécurité. Le but est d'identifier et d'analyser les risques pour les systèmes. Qu'est-ce que la « sécurité dès la conception » ? Quelles sont les mesures de sécurité existantes ? Nous nous intéresserons aussi à la protection de la chaîne logistique. Qu'est-ce qu'une chaîne logistique et quels sont les principaux risques du point de vue de la sécurité de l'information et les risques tels que les ransomware?

Le but est de comprendre les principes fondamentaux de la sécurité informatique et de pouvoir les appliquer.

Même si certains principes théoriques sont abordés, tels que la cryptographie, la gestion des accès, la protection des applications et des réseaux, etc., ce module se focalisera sur des exemples concrets et des check-lists.

Jour 4 : PM : Sécurité physique

Après-midi : sécurité physique

Ce module aborde les différents risques de sécurité physique et les mesures complémentaires de sécurité de l'information et de protection des données.

La sécurité physique est le pendant de la sécurité de l'information. Une clé USB avec des informations confidentielles qui est volée ou perdue peut constituer un problème majeur. Ou imaginez qu'un individu pénètre dans un centre de données sans autorisation. Des mesures de sécurité adéquates doivent être prévues à cet effet.

Le but est de comprendre le rôle de la sécurité physique et d'apprendre les bonnes pratiques à appliquer en matière de contrôle d'accès et de surveillance. Quelles sont les menaces physiques qui existent et quelles sont les mesures de sécurité à prendre à cet égard ?

Jour 5 : AM : Un aperçu des principales fuites de données de ces dernières années et de la manière dont elles ont été traitées

Matin : un aperçu des principales fuites de données et leçons à en tirer

Nous fournirons un aperçu des fuites de données des dernières années qui ont eu un impact important. Quels dommages ont-elles causé ? Comment les fuites de données ont-elles été détectées et ensuite traitées ? L'essentiel est d'apprendre à traiter les risques et à prendre des mesures préventives pour éviter de telles fuites de données. Est-ce possible et comment ? Les autorités de contrôle ont-elle été contactées et les personnes concernées ont-elles été informées ? Quelles sont les leçons à tirer de cette gestion d'incident ? Quelles sont les bonnes pratiques à retenir ?

Jour 5 : PM : **Business Continuity**

Après-midi : Business Continuity

L'élaboration d'un plan de continuité permet de réagir aux incidents qui mettent en péril la continuité de l'organisation. Ce module explique divers 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 permettra de comprendre le rapport entre la continuité d'une organisation et les diverses mesures associées.

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 consistent le business continuity (BCP) et le disaster recovery (DRP) ?

Jour 6 : AM : Intelligence artificielle et sécurité de l'information

Matin : L'IA et la sécurité de l'information

Le but est de comprendre l'impact du Règlement sur l'IA sur l'utilisation des systèmes d'IA dans les organisations. Il faut 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 les identifier et les évaluer ? Y a-t-il des risques à utiliser l'IA dans le traitement de données ? Existe-t-il des directives pour développer des logiciels 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 aborderons les principes de base de l'IA et la réglementation y afférente afin de pouvoir utiliser l'IA dans le traitement de données à caractère personnel de manière sûre et conforme à la loi.

Jour 6 : PM : Sécurité du cloud

Après-midi : Sécurité du cloud

Lorsqu'il s'agit de choisir une solution pour la gestion de l'information, le cloud s'avère être 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 : Session libre

Nous passerons en revue les différents concepts abordés dans les différents modules et répondrons à des questions complémentaires. Nous présenterons également une série de documents utiles dans le cadre de l'exercice de ce rôle.

Modalités d'inscription:

Le demandeur doit :

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

Prix

Le prix de la formation complète est de 1.750 euros.

Annulation et modifications

La participation peut être annulée jusque deux semaines avant le début de la session.

Smals se réserve le droit de modifier le programme de la formation.

Les inscriptions sont acceptées jusqu'à ce que le nombre maximum de participants soit atteint.