OPLEIDING TOT FUNCTIONARIS VOOR GEGEVENSBESCHERMING BINNEN DE SOCIALE ZEKERHEID EN GEZONDHEID

Doelstelling

De opleiding geeft u basisinformatie (inbegrepen tools) om het werk van een functionaris voor gegevensbescherming (DPO) binnen de sociale zekerheid en de gezondheid te kunnen uitvoeren. Naast enkele theoretische principes zal deze opleiding gericht zijn op de praktijk.

Ze wordt gegeven door experts inzake informatieveiligheid en gegevensbescherming die u met behulp van verschillende praktijk voorbeelden zullen uitleggen hoe zij hun werk uitvoeren.
Deze opleiding houdt rekening met de nieuwe regelgevingen (NIS, eIDAS, AVG, ...).

Op het einde van elke module zal er een evaluatie gevraagd worden om waar nodig bij te sturen. De inhoud van een module kan in die zin aan de opmerkingen van de deelnemers worden aangepast.

Methodologie

De opleiding omvat de verschillende delen van de rol van de DPO. De aanpak zal:
- Gebaseerd zijn op risicoanalyse, controles en tegenmaatregelen
- Toegespitst worden op de ervaring en de sector van de deelnemers
- Interactief (oefening, discussie, werk, ...) zijn om het begrip van de concepten te valideren
- Participatief zijn om de cursussen aan het publiek aan te passen/de oefeningen te animeren

Doelgroep

Deze opleiding richt zich tot de startende DPO's (en adjuncten) of zij die hun kennis in verband met de nieuwe wetten & reglementeringen willen bijschaven.

Inhoud van de opleiding

Dag 1: Inleiding, governance en de bescherming van de persoonsgegevens

Ochtend : Inleiding & governance

Deze opleiding zorgt ervoor dat we enerzijds de informatieveiligheid en gegevensbescherming begrijpen in het kader van de sociale zekerheid en gezondheid (wetten & reglementeringen over de informatieveiligheid en gegevensbescherming , de minimale normen) en anderzijds kennis verwerven over de governance inzake informatieveiligheid (ISMS, rollen en verantwoordelijkheden) en de rol van functionaris inzake informatieveiligheid en gegevensbescherming.

Namiddag : De bescherming van de verwerking van de persoonsgegevens (AVG)

Gedurende een halve dag presenteren we de belangrijkste thema's van de AVG regelgeving in verband met de bescherming van de verwerking van de persoonsgegevens en demonstreren we hulpmiddelen om deze regelgeving in de praktijk om te zetten.

Na deze dag bent u voorbereid om uw informatiebeveiliging te organiseren, te documenteren en te beheren en kan u de rol opstarten van functionaris voor gegevensbescherming of zijn/haar plaatsvervanger voor middelgrote organisaties.

Dag 2: Risicobeheer

Het doel van deze dag is een ondersteuning te bieden bij het formaliseren van de risico's en U te informeren over de best mogelijke manieren om deze risico's verder te verwerken binnen uw organisatie.

Op een interactieve manier zal de training het hele risicobeheerproces doorlopen, inclusief de opdeling van de verantwoordelijkheden in het proces, de risico identificatietechnieken met de gepaste antwoorden op de risico's .

De basis van de opleiding bestaat enerzijds uit de ISO 31000-norm voor risicobeheer van ondernemingen en anderzijds uit een informatiebeveiligingsoefening waarmee u de elementen die gedurende de dag worden gepresenteerd, kunt toepassen.

Er wordt ook bijzondere aandacht besteed aan het risicobeheer in projecten. Wij nodigen u uit om u voor te bereiden via een project van uw organisatie zodat u dit onderdeel optimaal kunt verwerken; dit kan zijn een IT project, een verhuizing, een vervanging van een belangrijk persoon, enz ... .

Dag 3: ICT technische veiligheid

Een groot deel van uw rol als DPO zal erin bestaan om de risico's te evalueren en om de informatietechnologieën en gegevens, gebruikt door uw organisatie, te beheren.
Deze module heeft niet als doel om een informaticus te worden of om te coderen, maar om de werkingsmechanismen te begrijpen zodat de juiste vragen gesteld worden in verband met de veiligheidsmaatregelen.

Hoewel bepaalde theoretische principes overlopen worden, zoals de cryptografie, beveiliging van applicaties en netwerken, ... zal deze module gericht zijn op concrete voorbeelden en checklists. De dag zal afgesloten worden met een kleine oefening om uw kennis te toetsen over dit technisch domein.

Dag 4: De fysieke veiligheid + bewustmaking

In deze module worden de verschillende fysieke veiligheidsrisico's en bijkomende maatregelen in verband met informatieveiligheid en gegevensbescherming aangehaald. Sensibiliseringscampagnes zijn hierbij een belangrijk onderdeel.

De fysieke veiligheid is de tweelingszus van de informatieveiligheid. Een USB-stick die gestolen wordt of verloren raakt met vertrouwelijke informatie kan een groot probleem vormen. Of stel u voor dat iemand uw datacenter binnen treedt zonder toelating. Hiervoor dient U voldoende beveiligingsmaatregelen te voorzien.

De eerste zwakke schakel blijft de mens. We moeten dus voortdurend de medewerkers sensibiliseren voor de "digitale" veiligheid. De dag zal afgesloten worden met een oefening waarbij er een sensibiliseringscampagne wordt opgesteld.

Dag 5 - Het beheer van veiligheidsincidenten + continuïteit

Ochtend : Het beheer van veiligheidsincidenten

Een proces om incidenten te beheren zorgt ervoor dat er minder paniek is wanneer een incident zich voordoet. Hierdoor kan u een gestructureerd en duidelijk antwoord bieden aan het gestelde probleem.

Namiddag : Continuïteit

Het opstellen van een continuïteitsplan maakt het mogelijk om te reageren op incidenten die de continuïteit van uw organisatie in het gevaar brengen. Deze module zal verschillende aspecten van het continuïteitsplan toelichten zoals een methodiek voor het uitvoeren van een ICT-DRP, de levenscyclus van de gegevens en de begrippen inzake back-up. Het zal u toelaten om de verbanden te begrijpen tussen de continuïteit van een organisatie en de verschillende gerelateerde maatregelen.

Dag 6: ***Privacy & security by design + CLOUD***

Ochtend : Privacy & security by design

De Algemene Verordening Gegevensbescherming (AVG) vereist dat de verwerkingsverantwoordelijke interne beleidsmaatregelen neemt door ontwerp en door standaardisatie. In deze module worden de verschillende concepten beschreven die U kunnen helpen bij de implementatie ervan en worden benaderingen voorgesteld om deze concepten te realiseren.

Namiddag : CLOUD

Bij de keuze van oplossingen om informatie te beheren, is de cloud een van de meest populaire oplossingen. Deze module helpt u te begrijpen wat een cloud is en illustreert de verschillende cloudmodellen. Tevens illustreren we hoe u de keuze van een cloud het best kunt benaderen om een antwoord te geven aan de verschillende beveiligingsrisico's.

Dag 7 : Samenvattende oefening

Tijdens deze dag worden de concepten die u in de verschillende modules hebt geleerd geoefend aan de hand van een voorbeeld uit de praktijk .

Inschrijvingsmodaliteiten

De aanvrager moet :

- werken bij een instelling die lid is van Smals
- een medewerker zijn van de informatieveiligheidsdienst binnen een instelling die deel uitmaakt van het netwerk van de sociale zekerheid en gezondheid

Prijs

De prijs voor de volledige opleiding is 1750 euro.

Annuleren & wijzigen

De deelname kan geannuleerd worden tot twee weken voor het begin van de sessie.
Smals behoudt zich steeds het recht om wijzigingen aan het opleidingsprogramma aan te brengen.
Inschrijvingen worden aanvaard tot het maximum aantal deelnemers bereikt is.