

# OPLEIDING TOT FUNCTIONARIS VOOR GEGEVENSBESCHERMING BINNEN DE SOCIALE ZEKERHEID EN GEZONDHEID

## Doelstelling

De opleiding geeft 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 ervaringsdeskundigen inzake informatieveiligheid en gegevensbescherming die met behulp van verschillende praktijkvoorbeelden zullen uitleggen hoe zij hun werk uitvoeren. Deze opleiding houdt rekening met de nieuwe regelgevingen (AVG, AI Act, NIS 2, ...).

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:

- inzichten verschaffen in de domeinen van 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: VM: Inleiding tot GDPR en informatieveiligheid

**Ochtend:** inleiding tot de GDPR, Privacy en informatieveiligheid en gegevensbescherming

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.

We maken kennis met de AVG en met enkele basisbegrippen zoals persoonsgegevens, vertrouwelijkheid, integriteit, beschikbaarheid, verwerking, verwerker, verwerkingsverantwoordelijke.

### Dag 1: NM: Rechten van betrokkenen

**Namiddag:** Rechten van betrokkenen

We gaan in op de rechten en plichten van de betrokkenen volgens de AVG en op de belangrijkste thema's van de AVG regelgeving in verband met de bescherming van de verwerking van de persoonsgegevens en we tonen hulpmiddelen om deze regelgeving in de praktijk om te zetten. We leren wat een DPO doet, wat zijn/haar wettelijke verplichtingen zijn. We gaan in op de rechten van betrokkenen en over omgaan met verzoeken van burgers. Verder hebben we het over het Data Protection Framework en de klokkenluidersregeling.

Op die manier kan de informatiebeveiliging worden georganiseerd, gedocumenteerd, beheerd en kan de rol worden opgestart van functionaris voor gegevensbescherming of zijn/haar plaatsvervanger voor middelgrote organisaties.

### Dag 2—: VM: Regelgeving in het kader van informatieveiligheid & gegevensbescherming

**Ochtend:** Regelgeving in het kader van informatieveiligheid en gegevensbescherming

We geven een overzicht van de relevante nationale en internationale regelgeving op het vlak van het digitale, financiële en gezondheidsdomeinen en hoe deze samenhangen. We leren de belangrijkste Europese en Belgische wetgevingen / regelgevingen begrijpen die een invloed hebben op data-en cybersecurity. Dit betreft onder meer ook de Data Act, de AI act, DORA, ...

We leren over de basisprincipes van NIS 2 en de cyberfundamentals en leren deze toepassen binnen een organisatie. We leggen uit wat informatieveiligheid inhoudt. Dit geeft ook de aanloop tot risicobeheer.

## Dag 2 : NM: Risicobeheer en beveiligingsmaatregelen (met inbegrip van DPbyD)

**Namiddag:** Risicobeheer en beveiligingsmaatregelen

Het doel van deze sessie is een ondersteuning te bieden bij het formaliseren van de risico's en te informeren over de best mogelijke manieren om deze risico's verder te verwerken binnen de 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 de elementen die gedurende de dag worden gepresenteerd, toegepast worden.

Er wordt ook bijzondere aandacht besteed aan het risicobeheer in projecten. Wij nodigen de deelnemers uit om een voorbereiding te maken van een project van de organisatie zodat dit onderdeel optimaal verwerkt wordt; dit kan zijn een IT project, een verhuizing, een vervanging van een belangrijk persoon, enz ... .

## Dag 3 : VM: Incidenten en datalekken

**Ochtend :** Het beheer van veiligheidsincidenten en datalekken

In een wereld waar digitalisering steeds verder toeneemt, worden organisaties in toenemende mate afhankelijk van hun IT-systemen. Tegelijkertijd groeit de hoeveelheid gevoelige gegevens die op deze systemen wordt opgeslagen exponentieel. Dit maakt organisaties kwetsbaar voor cyberincidenten en datalekken.

Deze dag zal de de context van cyberincidenten behandelen, de juridische implicaties, oorzaken van incidenten, en hoe organisaties effectief kunnen reageren middels detectie en incident response processen.

## Dag 3: NM: Beleid, Training & awareness (phishing, sensibilisering, ...)

**Namiddag:** Training en awareness

We leren hoe we een sterk informatieveiligheidsbeleid ontwikkelen en begrijpen. Hoe maken we medewerkers bewust van cyberrisico's en trainen we hen om bedreigingen te herkennen? Hoe zetten we het best een sensibiliseringscampagne op rond phishing en andere aanvallen, en counteren we social engineering technieken? Ook gaan we dieper in op de gevolgen van ransomware. Welke technieken gebruiken de aanvallers en hoe kunnen we ons hiertegen beschermen?

## Dag 4 : VM : Operationele veiligheid

**Ochtend:** operationele veiligheid

Een groot deel van de rol als DPO zal erin bestaan om de risico's te evalueren en om de informatietechnologieën en gegevens, gebruikt door de 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. We leren de risico's voor systemen identificeren en analyseren. Wat houdt security by Design in? Welke beveiligingsmaatregelen zijn er? We leren over de beveiliging van de supply chain. Wat houdt een supply chain in en wat zijn de voornaamste risico's vanuit het standpunt van informatiebeveiliging en vanuit de risico's zoals bijvoorbeeld ransomware.

We leren de fundamentele principes van ICT-beveiliging begrijpen en toepassen.

Hoewel bepaalde theoretische principes overlopen worden, zoals de cryptografie, toegangsbeheer, beveiliging van applicaties en netwerken, ... zal deze module gericht zijn op concrete voorbeelden en checklists.

## Dag 4 : NM : Fysieke veiligheid

**Namiddag:** fysieke veiligheid

In deze module worden de verschillende fysieke veiligheidsrisico's en bijkomende maatregelen in verband met informatieveiligheid en gegevensbescherming aangehaald.

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 wanneer iemand een datacenter binnen treedt zonder toelating. Hiervoor dienen er voldoende beveiligingsmaatregelen voorzien te worden.

We leren de rol van fysieke beveiliging begrijpen en leren over de best practices die we toepassen voor toegangscontrole en bewaking. Welke fysieke dreigingen zijn er en welke beveiligingsmaatregelen kunnen we hiervoor nemen?

## Dag 5 : VM: Een overzicht van de grootste datalekken van de voorbije jaren en hoe ze werden behandeld

**Ochtend:** een overzicht van de bekendste datalekken en wat we hieruit kunnen leren

We geven een overzicht van de datalekken van de voorbije jaren, die een grote impact hadden. Welke schade werd aangericht ? Hoe werden de datalekken gedetecteerd, en nadien opgevolgd ? Belangrijk is het leren behandelen van de risico's en het nemen van preventieve maatregelen om zulke datalekken te vermijden. Is dit mogelijk en hoe ? Werden toezichthouders gecontacteerd en betrokkenen geïnformeerd? Wat kunnen we leren uit dit incidentbeheer ? Welke best practices nemen we mee ?

## Dag 5 : NM : Business Continuity

**Namiddag :** Business Continuity

Het opstellen van een continuïteitsplan maakt het mogelijk om te reageren op incidenten die de continuïteit van de 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 toelaten om de verbanden te begrijpen tussen de continuïteit van een organisatie en de verschillende gerelateerde maatregelen.

We leren om de impact (op het vlak van confidentialiteit, integriteit en beschikbaarheid) van veiligheidsincidenten en cyberaanvallen op de continuïteit in te schatten. Wat houdt business continuity (BCP) en de disaster recovery (DRP) in ?

## Dag 6: VM: Artificial Intelligence en informatieveiligheid

**Ochtend:** AI en informatieveiligheid

We leren om de impact van de AI act op het gebruik van AI-systemen in organisaties te begrijpen. We moeten leren om relevante vragen te stellen. Wat zijn de risico's van AI ? Wat is de kans op incidenten bij het gebruik van AI ? Hoe leren we om deze te identificeren en te evalueren ? Zijn er risico's als we AI gebruiken bij gegevensverwerking ? Zijn er richtlijnen die we kunnen toepassen bij een veilige ontwikkeling van AI-software ? We leren best practices kennen voor machine-learning beveiliging en de software supply chain.

We leren de basisprincipes van AI en de desbetreffende regelgeving om AI veilig en conform de wetgeving in te zetten bij de verwerking van persoonsgegevens.

## Dag 6: NM : Cloud Security

**Namiddag:** Cloud security

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

We leren onder meer over de verschillende cloudmodellen, hun risico's en de beveiligingsprincipes van cloud computing.

## Dag 7 : Open sessie

We geven een overzicht over de concepten in de verschillende modules en geven een antwoord op bijkomende vragen. Vervolgens overlopen we ook een aantal documenten in dit kader die gebruikt kunnen worden in de uitoefening van deze rol.

### **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.