

# certified dpo (gdpr): functionaris gegevensbescherming (avg)

€ 1300,00 excl. BTW

I.S.M. 

## omschrijving

### INTRODUCTIE

In mei 2018 ging de nieuwe **Algemene Verordening Gegevensbescherming (AVG)** of misschien nog beter gekend als GDPR (General Data Protection Regulation) juridisch van kracht. Deze AVG (of GDPR) heeft tot doel natuurlijke personen de controle over hun persoonsgegevens terug te geven door nieuwe geactualiseerde spelregels op te leggen betreffende het verzamelen en beheeren van deze persoonsgegevens. Openbare besturen maar ook organisaties uit de social profit die zich - na mei 2018 - niet houden aan deze nieuwe regelgeving kunnen door de gegevensbeschermingsautoriteit of kortweg: "GBA" (voorheen privacy commissie) belangrijke sancties opgelegd worden.

Zowel lokale besturen (steden, gemeenten, OCMW's, agentschappen, federale overheden...) maar ook social profit organisaties verzamelen persoonsgegevens over hun "klanten", prospecten of burgers om bvb. betere inzichten te verwerven betreffende huidige of toekomstige behoeften. Om het verzamelen en vervolgens het verwerken van persoonsgegevens correct - volgens de GDPR wetgeving - te laten verlopen is elke organisatie verplicht een '**DPO**' of '**Functionaris gegevensbescherming**' aan te stellen. Opdat deze Data Protection Officer (of DPO) met kennis van zaken zijn of haar jobrol zou kunnen vervullen, is een gedegen basisopleiding een eerste noodzakelijke stap om volgens een structurele aanpak aan de minimum GDPR vereisten te kunnen voldoen.

### OMSCHRIJVING

Deze opleiding heeft als doel deelnemers op te leiden tot '**Certified DPO (GDPR)**' of '**Gecertificeerde functionaris gegevensbescherming**'. Na het volgen van deze opleiding en succesvol afleggen van het examen (laatste lesdag) beschikt de deelnemer over voldoende theoretische kennis om de eerste stappen te zetten als DPO.

Deze vernieuwde opleiding is een pragmatische mix afkomstig uit 3 verschillende kennisdomeinen - juridisch, IT security technologie en proces- en projectmanagement - die dan ook tijdens de opleiding uitgebreid aan bod komen. De opleiding is gericht op het verwerven van een gedegen theoretische basiskennis geschoeid op de leest van alle relevante generieke processen die binnen elk openbaar bestuur (lokaal, Vlaams of federaal...) of elke social profit aanwezig zijn.

Om deze opleiding aan te vatten hoeft u dan zeker geen IT-er of jurist te zijn, maar organisatiekunde of procesmatig denken en sectorale kennis zijn troeven om uw slaagkansen tot het behalen van het '**Certificaat DPO (GDPR): Functionaris gegevensbescherming (AVG)**' te maximaliseren.

Met het behalen van dit certificaat bewijst de deelnemer over de minimum nodige theoretisch kennis te beschikken om de eerste stappen te kunnen zetten als Data Protection Officer (of 'DPO') of 'Functionaris gegevensbescherming'.

Uit ervaring blijkt echter dat deelnemers die deze opleiding hebben gevolgd er baat bij hebben om de vervolg opleiding '**DPO in de praktijk**' te volgen. Via de combinatie van deze 2 opleidingen zijn de deelnemers volledig gewapend de verworven kennis uit deze opleidingen om te zetten in heel praktijkgericht actieplan.

### **Maak van de nood een deugd!**

Gezien deze nieuwe GDPR (AVG) wetgeving gevolgen zal hebben op oa de **organisatieprocessen ('Security & Privacy by Design & by Default')** zou deze nieuwe wetgeving als een 'last' kunnen aanzien worden. Echter bestaan er reeds een aantal voorbeelden van besturen of social profit organisaties die deze nieuwe wetgeving als een **opportuniteit** aangrijpen om nauwer met hun klanten of burgers in dialoog te treden door hen oa. duidelijk uit te leggen waarom bepaalde informatie wordt bijgehouden. Dergelijke - soms verrassende - use cases komen in deze opleiding ook aan bod en hebben tot doel deelnemers te inspireren om een hogere toegevoegde waarde na te streven als extra service laag bovenop deze wettelijk verplichting.

### VOOR WIE IS DEZE OPLEIDING BESTEMD?

- Aspirant Data Protection Officer

- Informatiebeheerders of afdelingshoofden
- Juristen met de ambitie om DPO te worden
- Risk Managers, Security verantwoordelijken

#### VOORKENNIS

Kennis van organisiestieprocessen, informatiestromen, binnen eigen organisatie of openbaar bestuur.

#### METHODOLOGIE

De volledige opleiding is 'doorspekt' met **praktijkvoorbeelden** van de belangrijkste informatiestromen waarin informatie over persoonsgegevens kunnen voorkomen en waaraan aandacht dient besteed te worden **binnen de context van 'GDPR wetgeving'**.

Door deze aanpak krijgen de deelnemers stap voor stap de nodige inzichten en feeling betreffende de wijze waarop deze op het eerste zicht 'saai ogende materie' in dient toegepast te worden.

Hands-on leren werken met de online Informatieveiligheidstool [www.informatieveiligheid.be](http://www.informatieveiligheid.be)

Vanaf de 1ste lesdag dient elke deelnemer zijn/haar laptop mee te brengen. Deelnemers zullen tijdens de opleiding leren werken met deze Informatieveiligheidstool met als doel:

- Risicoanalyses en maturiteitsmetingen te voltrekken
- Veiligheidsplannen te genereren via de tool

Vanaf de laatste lesdag krijgt elke deelnemer gedurende **één maand gratis toegang tot de standaard versie** van deze tool.

## programma

### Module 1: Het wettelijk GDPR kader: duiding en inspirerende use cases informatieveiligheid.

Sinds de richtlijn van 1995 (95/46/EG) heeft onze informatiemaatschappij een onwaarschijnlijke vlucht genomen. Met de opkomst van het internet, zoekmachines, social media, mobile devices en allerhande internetdiensten is het aantal informatiebronnen exponentieel gestegen. We leven op en top in een informatiemaatschappij waarbij de gemiddelde "burger" tientallen digitale identiteiten - al of niet bewust - heeft aangemaakt waarbij men in minstens evenveel databanken persoonlijke gegevens heeft achtergelaten, en waardoor men de controle over de persoonlijke gegevens is kwijtgeraakt. Hierdoor wordt de "burger" vanuit alle hoeken soms belaagd met ongewenste informatie waarbij men zich soms afvraagt hoe dit zo ver is kunnen komen. Deze **nieuwe Europese GDPR regelgeving (of AVG)** heeft als doel elk natuurlijk persoon de controle over zijn/haar persoonsgegevens terug te geven. Deze module gaat dieper in op dit nieuwe wettelijke kader en hoe deze regelgeving dient geïnterpreteerd en toegepast te worden. Op het einde van deze module worden de deelnemers ook geïnspireerd om van deze nieuwe wetgeving een mogelijke unieke selling proposition (USP) te maken.

#### a) Het brede wettelijke kader GDPR - AVG - Verordening (EU) 2016/679

- Korte historische duiding - Helicopterview context
  - Noodzaak voor aanpassing van wetgeving
  - Doelstelling van GDPR - AVG - Verordening (EU) 2016/679?
  - GDPR versus met de Richtlijn 95/46/EG
- De rol, verantwoordelijkheden en taken van een functionaris voor gegevensbescherming
- De rol en verantwoordelijkheden van het managementteam van een KMO tov functionaris voor gegevensbescherming' op basis van GDPR (AVG)

#### b) De GDPR artikels op een praktische en pragmatische wijze bekeken:

- Algemene bepalingen en beginselen
- Rechten van de betrokkene
- Verwerkingsverantwoordelijke en verwerker
- Doorgifte van persoonsgegevens aan derde landen of internationale organisaties
- Onafhankelijke toezichhoudende autoriteiten
- Samenwerking en coherentie
- Beroep, aansprakelijkheid en sancties
- Bepalingen in verband met specifieke situaties op het gebied van gegevensverwerking

- Gedelegeerde handelingen en uitvoerende handelingen
- Slotbepalingen

**c) De drie domeinen die moeten geactiveerd, beheerd en gemonitord worden om 'GDPR Compliance' te realiseren:**

- Processen, (zie ook module 2 en 4)
- ICT-technologie, (zie ook module 3)
- Mensen, (zie module 2, 3, 4)

**d) GDPR: van de nood een deugd (of een USP) maken (zie ook module 5)**

Extra waarde creatie naar de klant toe als extra 'service laag' bovenop GDPR

- Inspirerende Use Cases (= deel 1, zie ook module 5 voor deel 2)
- Ondersteunende modellen om strategische business waarde te creëren:
  - Introductie Business Model Canvas (BMC)
  - Introductie Value Proposition Canvas (VPC)

**Module 2: Pragmatische vertaalslag van het wetgevend kader naar een 'GDPR Informatieveiligheidsframework'**

De ideale wereld bestaat niet, dé ideale oplossing evenmin! Dit informatieveiligheidsframework werd opgebouwd op basis van gespreken met security experts, informatieveiligheidsconsulenten, professionals uit het werkveld én op basis van bestaande Informatieveiligheidsstandaarden en best practices (oa ISO27000 series) - en heeft tot doel een overkoepelend 'GDPR informatieveiligheidsframework' aan te reiken waarmee (toekomstige) functionarissen gegevensbescherming of "DPO-ers" op een praktijkgerichte wijze mee aan de slag kunnen om oa een Informatieveiligheidsplan op te bouwen.

**a) Belangrijke bouwstenen voor de opbouw van een Information Security Management Framework om te komen tot een Informatie Security management System (ISMS):**

- Het '13 stappenplan (AVG)' én 'Privacy op de werkvloer' door Privacy Commissie
- 'CODEX - Algemene verordening gegevensbescherming' door Dirk De Bot (Politeia)
  - ISO27000 series als overkoepelend framework voor het opzetten (of aanpassen van een bestaand) ISMS ifv GDPR (AVG) compliance:
  - De mapping van GDPR (AVG) met ISO27000 series
  - Richtlijnen om ISO27000 series toe te passen om ISMS op te zetten
  - Richtlijnen voor aanpassing bijsturing voor bedrijven die reeds ISO27000-series toepassen,
  - Stap voor stap aanpak om een ISMS op te zetten
  - Introductie tot opmaak van een 'informatie privacy plan én informatieveiligheidsplan' (verdere uitdieping module 5)

**b) Pragmatische vertaalslag van wettelijk GDPR kader naar informatieveiligheidsframework: streven naar een ideale wereld met behulp van 'Security én Privacy by Design en by Default':**

- Binnen bestaande bedrijfsprocessen en informatiesystemen (oa software applicaties, ...)
- Opleggen als business requirements voor nieuw te bouwen (of aan te passen) informatiesystemen (oa software applicaties,...)

**c) Introductie opbouw van een informatieveiligheidsplan om te komen tot 'GDPR Compliance'**

**Module 3: De ondersteunende rol van ICT om de naleving van GDPR te realiseren.**

ICT technologie is - naast processen en mensen - één van de drie domeinen die een belangrijke ondersteunende rol kan spelen om een informatieveiligheidsplan in praktijk om te zetten. Deze module heeft als doel een overzicht en inzicht te bieden in de domeinen waar ICT kan worden ingezet ifv 'GDPR Compliance'.

Wat is kan aanzien worden als 'security bedreiging' binnen de context van Data breaches die schadelijke gevolgen kunnen hebben voor organisatie/bedrijf:

- Feiten en cijfers
- Situering aan de hand van praktijkvoorbeelden en korte analyse wat de oorzaak was van deze data breaches

**a) Register van verwerkingsactiviteiten**

**b) Gegevensbeschermingseffectbeoordeling**

**c) Technische en organisatorische maatregelen:**

- Logische toegangsbeveiliging
  - Strategie

- AAA (Authenticatie, Autorisatie, Accounting)
- Pseudonimisering en versleuteling
- IT maatregelen om de continuïteit te garanderen
  - Begrippen
  - Strategieën
- Bescherming van het netwerk
  - Begrippen
  - Strategieën
- Bescherming tegen malware
  - Soorten
  - Maatregelen
- Personeel (IT-adviezen, richtlijnen)
  - Wachtwoordbeleid
  - Rapportering incidenten
  - Bewustwording
- Herstel gegevens (back-up's)
  - Begrippen
  - Strategieën

#### **d) Evaluatie technische maatregelen:**

- Bewaking vertrouwelijkheid, integriteit en beschikbaarheid (monitoring & logging)
- Security audits (Kwetsbaarheidsscans en pentesten)

#### **e) Rechten van de betrokkene (technische vertaling):**

- Het recht om vergeten te worden
- Het recht om gegevens op te vragen

#### **f) Datalekken:**

- Beleid
- Actieplan
- Rapportering

### **Module 4: Afdwingen en bewaken van naleving GDPR via project-, proces- en IT service management.**

Opdat bedrijven en zelfs openbare besturen een goede dienstverlening zouden kunnen blijven garanderen worden zij steeds meer 'aangestuurd' door opportuniteiten/projecten waardoor zij bijna continu in verandering zijn. En daar heel wat projecten te maken hebben met het verhogen van de 'informatievloeibaarheid' doorheen het bedrijf - aangestuurd door de zoektocht naar waarde creatie voor de klant - dient ook rekening gehouden te worden met privacy issues en informatieveiligheid.

Projecten op zich houden steeds een verhoogd risico in net omdat projecten per definitie afwijken van 'Business as Usual' die gebaseerd is op ingeburgerde bedrijfsprocessen die (hopelijk) reeds GDPR Compliant zijn. Ook bij projecten dient men reeds in de beginfase rekening te houden met 'Security & Privacy by design & by default' zodanig dat 'GDPR Compliance' ingebakken zit binnen in projectprocessen. Bij de aanvang (by design) van een project is het zaak rekening te houden met de richtlijnen betreffende Informatieveiligheid die beschreven staan in het ISMS van het bedrijf. Beschikt een bedrijf nog niet over een 'Information Security Management System (ISMS)' dan is het opstellen van een ISMS een belangrijk actiepunt om dit organisatie breed te ontwikkelen en te implementeren. Vervolgens is het ook belangrijk dat de gewijzigde (of nieuwe) bedrijfsprocessen worden opgenomen in een bestaand 'Incident Management Systeem (ISM)'. Echter is de kans ook hier groot dat niet alle bedrijven, organisaties of besturen nu reeds over een ISMS beschikken. Er bestaan echter in de markt voldoende tools die op een eenvoudige wijze hiervoor een oplossing kunnen bieden.

Deze module heeft zowel als doel een best practice aan te bieden rond risicomanagement en projectmanagement methodes als rond (IT) Service management en hoe deze kunnen gebruikt worden in de aanpak naar de opzet van een ISMS.

#### **a) Risico management methodes:**

- gaande van een management risico-analyse
- tot een meer gedetailleerde risico analyse aanpak op proces/dienstniveau

#### **b) Projectmanagement methodes:**

- Algemene methodes: Prince2, PMBok
- Methodes gericht op Software ontwikkeling: Agile, Scrum, Secure Software Design

### c) IT Service Management (ITIL):

- Wat is ITIL?
- Hoe kan ITIL helpen bij het opzetten van Incident Management System (IMS) of een incidenten register
- Overzicht Software ivm IMS

### d) Aanpassen of opzetten van een Information Security Management System (ISMS):

- Wat is ISMS
- Wat is het doel van ISMS
- Hoe in de praktijk toepassen

### Module 5: Naleving GDPR/AVG toegepast in de praktijk (inclusief certificatie examen)

Per domein leert men werken met de online informatieveiligheidstool waarbij men risicoanalyses, maturiteitsmetingen en informatieveiligheidsplannen leert op te maken die gebaseerd zijn op het 'GDPR informatieveiligheidsframework':

- GDPR van de nood een deugd (of een USP) maken (zie ook module 1)
  - Interne plan van aanpak
  - Extra waarde creatie naar de klant toe als extra 'service laag' bovenop GDPR/AVG
  - Aanvullende Inspirerende Use Cases (deel 2, zie ook module 1 voor deel 1)
- Leren werken informatieveiligheidstool:
  - Risicometing
  - Maturiteitsmeting
  - Actieplan / veiligheidsplan
  - Interne samenwerking rond informatieveiligheid en bescherming van de persoonsgegevens

**Op het einde van de laatste lesdag (= op het einde van module 5) leggen de deelnemers het officiële examen af.**

## praktisch

Deze opleiding wordt georganiseerd door onze partner SBM, cvba Skilliant.

| LESDATA             |          |         | LOCATIE                                      | CONTACT  |
|---------------------|----------|---------|--|--|
| DATUM               | STARTUUR | EINDUUR | SBM Gent<br>Tramstraat 63<br>9052 Zwijnaarde | T: 078 35 39 30<br>F: 051/268754<br>info@escala.be |
| woensdag 06/11/2019 | 09:00    | 12:00   |  |  |
| woensdag 06/11/2019 | 13:00    | 16:00   |  |  |
| woensdag 13/11/2019 | 09:00    | 12:00   |  |  |
| woensdag 13/11/2019 | 13:00    | 16:00   |  |  |
| woensdag 20/11/2019 | 09:00    | 12:00   |  |  |
| woensdag 20/11/2019 | 13:00    | 16:00   |  |  |
| woensdag 27/11/2019 | 09:00    | 12:00   |  |  |
| woensdag 27/11/2019 | 13:00    | 16:00   |  |  |
| woensdag 04/12/2019 | 09:00    | 12:00   |  |  |
| woensdag 04/12/2019 | 13:00    | 16:00   |  |  |

Data onder voorbehoud van eventuele wijzigingen.

## docent

**Eddy Van der Stock**, Voorzitter van Vlaamse ICT organisatie VZW (V-ICT-OR) en president van de wereldwijde internationale Linked Organisation of Local Authorities NPO (LOLA).

**Gespecialiseerd in:**

- BPM, projectmanagement
- Informatie security (lead auditor) en riscomanagemen
- Intergouvernementele projectbegeleiding
- Initiëren, begeleiden van werkgroepen en think-tank ontwikkeling rond de moderne dienstverlening en de rol van ICT binnen openbare besturen van de toekomst

**partners**

In samenwerking met Vlaamse ICT Organisatie [www.v-ict-or.be](http://www.v-ict-or.be) academy