Duthler Academy
Kennis, groei & verandering

Studieprogramma

Opleiding Functionaris voor Gegevensbescherming (FG)

Versie 1.1, 4 februari 2026

Opleiding functionaris voor gegevensbescherming (FG)

De AVG heeft de Functionaris voor Gegevensbescherming (FG) aangewezen als de onafhankelijke interne toezichthouder. De FG adviseert en informeert de organisatie en is aanspreekpunt voor betrokkenen en de toezichthouder.

Om de functie van FG goed uit te kunnen oefenen moet een FG beschikken over bovengemiddelde vakkennis en vaardigheden op het gebied van privacywetgeving en de praktijk van gegevensbescherming.

Daarnaast is kennis nodig van aanverwante onderwerpen zoals cyberbeveiliging en Artificial Intelligence (AI).

De Opleiding FG biedt naast juridische kennis ook praktische vaardigheden. Denk aan het treffen van beheers- en beveiligingsmaatregelen en het organiseren van compliance met wettelijke en contractuele verplichtingen.

De Opleiding FG sluit aan bij de kwaliteitseisen en de gedragscode van het Nederlands Register voor Functionarissen voor Gegevensbescherming (NRFG).

Vanuit een persoonlijke leeromgeving heeft de deelnemer toegang tot de cursussen die behoren tot de Opleiding FG. In de leeromgeving is de literatuur te vinden en kunnen toetsen worden gemaakt. Dat is niet alleen de eindtoets van elke cursus maar ook een diagnostische toets waarmee een deelnemer zijn of haar kennisniveau kan testen.

Tijdens een workshop van 4 uur lichten de docenten de theorie nader toe, behandelen zij een casus en bespreken zij praktijkvoorbeelden. Er is alle ruimte is voor het stellen van vragen. Na het volgen van de workshop kan de deelnemer vanuit de eigen leeromgeving een toets maken. Vanuit de leeromgeving koppelt de docent de resultaten vervolgens aan de deelnemer terug.

Na het succesvol afronden van de toets blijft de cursus voor de deelnemer beschikbaar. De docenten onderhouden de cursus zodat er altijd toegang is tot een cursus die actueel is.

De Opleiding FG bestaat uit 12 cursussen die zijn onderverdeeld in de categorieën “Formeel Juridisch”, “Governance & Compliance”, “Organiseren van bedrijfsactiviteiten” en “Assessment & Audit”.

Cursusonderwerpen	
A	**Formeel Juridisch**

1. Overzicht huidige privacywet- en regelgeving

In deze cursus krijgt de cursist een overzicht van de huidige privacywetgeving. Wij beginnen met de Europese Algemene verordening gegevensbescherming (AVG) en noemen aanpalende wetgeving. Wij gaan in op de basisbegrippen, de beginselen en de uitgangspunten van de AVG, de verschillende (privacy)rollen in een organisatie, de belangrijkste rechten van betrokkenen en verplichtingen van verwerkingsverantwoordelijken en verwerkers van persoonsgegevens.

De AVG vormt de basis van alle privacywet- en regelgeving. Kennis hebben van de beginselen en van basisbegrippen is van groot belang om de AVG en de aanpalende wet- en regelgeving in de praktijk toe te kunnen passen. Aanpalende privacywet- en regelgeving vormen soms een aanvulling op de rechten en verplichtingen uit de AVG, soms komen zij in de plaats ervan.

De cursus is een eerste kennismaking met het primaire doel van de AVG, namelijk het centraal stellen van de betrokkene die de regie krijgt over zijn eigen persoonsgegevens en de wijze waarop de AVG dat heeft geconcretiseerd en uitgewerkt in rechten en verplichtingen. De cursist legt een fundament voor het opbouwen van kennis voor het organiseren van het beschermen van persoonsgegevens in een bedrijf of instelling.

2. Jurisprudentie, besluiten en richtlijnen

De AVG werd in 2016 van kracht en in 2018 van toepassing. In de tussentijd hebben toezichthouders gehandhaafd en is er jurisprudentie ontstaan die de uitleg van de rechten van betrokkenen en de verplichtingen van verwerkingsverantwoordelijken en verwerkers van persoonsgegevens nader verklaren.

Wij nemen belangrijke jurisprudentie, boetebesluiten en richtsnoeren van toezichthouders met de cursisten door en duiden deze. Wij geven aan wat de impact van de jurisprudentie, boetebesluiten en richtsnoeren is op de rechten en verplichtingen van betrokkenen en verwerkingsverantwoordelijken en verwerkers. Er ontstaat een overzicht van discussiepunten en uitleg waarmee bedrijven bij het organiseren van passende beheersmaatregelen gericht op het beschermen van persoonsgegevens rekening kunnen houden.

Privacyrecht bestaat niet alleen uit wet- en regelgeving. Om kennis over privacywetgeving actueel te houden is het regelmatig bestuderen van uitspraken jurisprudentie, besluiten en richtsnoeren essentieel.

3. Toezicht en handhaving van de AVG

In de AVG en de uitvoeringswet AVG hebben toezichthouders taken en bevoegdheden gekregen om de naleving van de AVG te bevorderen en zo nodig te handhaven. De AVG kent als interne toezichthouder de Functionaris voor Gegevensbescherming (FG). De externe toezichthouder is in Nederland de Autoriteit Persoonsgegevens (AP). De positie, taken en bevoegdheden van de FG zijn voornamelijk in de AVG zelf belegd. De positie, taken en bevoegdheden van de AP zijn behalve in de AVG zelf, ook in de Uitvoeringswet AVG en in de Algemene wet bestuursrecht geregeld.

In deze cursus gaan we in op de toezichtstaak van de FG en hoe deze in de praktijk kan worden vormgegeven in de organisatie van de verwerkingsverantwoordelijke en de verwerker. Daarnaast besteden we uitgebreid aandacht aan de taken en bevoegdheden van de AP. Op welke wijze oefent de AP toezicht uit en over welk handhavingsinstrumentarium beschikt zij? Wat houden de boetebeleidsregels in? Wat zijn de rechten en plichten van een organisatie als de AP bijvoorbeeld inlichtingen vordert of toegang tot IT-systemen? Hoe ver gaat de medewerkingsplicht? En wat is de verhouding tussen de FG en de AP op die momenten?

Naast theoretische kennis nemen wij u mee in de wijze waarop de AP tot nu toe in de praktijk uitvoering heeft gegeven aan haar taken en haar toezichts- en handhavingsbevoegdheden heeft toegepast. Ook staan wij stil bij de Europese collega's van de AP en hoe zij onderling met elkaar samenwerken.

4. De AVG in internationaal perspectief: Europa en doorgifte naar derde landen

In de cursus bespreken wij de formeel-juridische basis van de toepassing van de AVG in Europa zelf alsook in geval van doorgifte naar derde landen.

Wij bespreken de kaders waarbinnen de AVG tot stand is gekomen. Ook gaan wij in op de relatie met het EVRM en het Verdrag van Straatsburg en de verschillende manieren waarop rechtsbescherming kan worden gezocht. De rechtsgang naar het Europese Hof van Justitie en het Europese Hof voor de Rechten van de Mens wordt toegelicht aan de hand van enkele recente uitspraken. Ook komt aan de orde hoe het toezicht op Europees niveau is geregeld.

De AVG beoogt een uniform niveau en wijze van bescherming van persoonsgegevens in alle lidstaten van de EU. Omdat de verwerking van persoonsgegevens niet altijd of liever gezegd meestal niet beperkt is tot de grenzen van de EU, stelt de AVG voorwaarden voor doorgifte van persoonsgegevens vanuit de EU naar derde landen.

Gemeenschappelijke noemer van deze voorwaarden is dat in de derde landen een met de AVG vergelijkbaar beschermingsniveau vereist is om persoonsgegevens aan deze derde landen te mogen doorgeven.

In deze cursus bespreken we wat de voorwaarden en eisen concreet inhouden en hoe organisaties daaraan kunnen voldoen. We gaan in op adequaatheidsbesluiten, passende waarborgen, zoals binding corporate rules, gedragscodes en modelcontracten en specifieke uitzonderingen. We bespreken guidelines waarin deze voorwaarden verder zijn genuanceerd en staan stil bij een Data Transfer Impact Assessment (DTIA). In een DTIA brengen organisaties de risico's in kaart van gegevensdoorgifte naar derde landen, op een vergelijkbare wijze als bij een DPIA.

Wij bespreken aan de hand van een casus van een internationaal opererend bedrijf wat doorgifte naar een derde land concreet betekent en wat hier in de praktijk bij komt kijken.

5. Privacy en aanpalende nationale en internationale wetgeving

De AVG staat niet op zichzelf. In aanpalende wet- en regelgeving zijn bepalingen opgenomen, die enerzijds een uitwerking vormen van de AVG. Zo zijn in ministeriële besluiten grondslagen opgenomen, die een verwerking rechtmatig maken of bewaartermijnen die een nadere invulling geven aan het beginsel van dataminimalisatie. Anderzijds vormen deze aanpalende wet- en regelgeving een aanvulling op de AVG. Zonder kennis van deze aanpalende wet- en regelgeving wordt het lastig om toepassing te geven aan de AVG. Ook kennen we wet- en

regelgeving die in de plaats komt van bepalingen van de AVG. In deze cursus gaan we in op de meest relevante nationale aanpalende wet- en regelgeving.

Er is ook Europese wet- en regelgeving die vanuit andere perspectieven zoals de razendsnelle ontwikkelingen rond Artificial Intelligence (AI), de marktmacht van grote technologiebedrijven en de dreiging van cybercrime, bescherming van persoonsgegevens reguleert. Denk aan de Digital Services Act (DSA), de AI Act, de Network and Information Security Directive (NIS2) en de eIDAS-verordening. De verordeningen hebben rechtstreekse werking in alle lidstaten van de EU. De richtlijnen zijn of worden omgezet in nationale wetgeving.

In deze cursus bespreken wij hoe een bedrijf het relevante wettelijke kader kan bepalen en kan toepassen. De cursisten leren uit het relevante wettelijk kader de verplichtingen en aandachtspunten voor de bedrijfsactiviteiten van hun eigen bedrijf of organisatie af te leiden. Ook leert de cursist de samenhang tussen de AVG en de aanpalende Europese en internationale wetgeving te onderkennen en toe te passen. Zo kennen ook de NIS2-richtlijn en eIDAS-verordening meldplichten van cyberincidenten bij verschillende autoriteiten en binnen verschillende tijdskaders.

B Governance & Compliance

6. De FG: positie, taken, bevoegdheden en verantwoordelijkheden

De wetgever introduceert in de artikelen 37 – 39 AVG de rol van Functionaris voor Gegevensbescherming (FG), de toezichthouders (EDPB) werken de rol van de FG uit in hun *guidelines* en rechters genereren jurisprudentie waaruit blijkt wat de taakopvatting van de FG moet zijn. De taken, bevoegdheden en verantwoordelijkheden van de FG zijn redelijk duidelijk.

Als een persoon de rol van FG wil vervullen dan is het essentieel dat deze persoon de taken, bevoegdheden en verantwoordelijkheden kent. De verwerkingsverantwoordelijke of verwerker zal in de aanstellingsbrief van de FG de rol nauwgezet uitwerken en de FG zal beoordelen in hoeverre hij of zij de taken binnen de verstrekte bevoegdheden kan vervullen. Is de rolopvatting te veel ingesnoerd dan is de FG “vleugellam”; is de rolopvatting te ruim geformuleerd dan ervaart de organisatie de FG als een “lastpak”. Voor de persoon is de beschrijving van de rolopvatting essentieel voor het adequaat kunnen vervullen van de wettelijke taak van FG.

In deze cursus werken wij aan de hand van wetgeving, *guidelines*, jurisprudentie en maatschappelijke opinies de taakopvatting van de FG uit. Wij belichten het perspectief van de FG, de verwerkingsverantwoordelijke en de verwerker. In de workshop leggen wij een aantal casussituaties aan de cursisten voor en maken afwegingen. De ervaring leert dat er al snel ethische vraagstukken opkomen, die wij niet uit de weggaan en zullen bespreken.

7. Cyberbeveiliging en cyberhygiëne

Organisaties moeten steeds meer kennis hebben van informatiebeveiliging of ook wel cyberbeveiliging en aandacht besteden aan de interne cyberhygiëne. De digitale dreigingen nemen in rap tempo toe. We zijn allemaal met elkaar verbonden. Als een bedrijf of organisatie de cyberbeveiliging niet op orde heeft, dan is de kans groot dat bij een cyberaanval niet alleen bedrijfsgevoelige informatie, maar ook persoonsgegevens buit gemaakt worden.

Vanuit de AVG is er de verplichting om passende technische en organisatorische maatregelen te nemen om persoonsgegevens te beschermen. Vanuit de NIS2-richtijn en de Cyberbeveiligingswet is er de zorgplicht die organisaties dwingt om maatregelen te nemen om de netwerk en informatiesystemen te beschermen, die worden gebruikt voor de werkzaamheden en de dienstverlening van de organisatie. Eén van deze maatregelen is het implementeren van basispraktijken op het gebied van cyberhygiëne, zodat medewerkers en andere werkzame personen zich bewust zijn van beveiligingsrisico's en van het belang van digitaal weerbaarheid.

In deze cursus wordt de FG meegenomen in de wereld van cyberbeveiliging en cyberweerbaarheid. Wat zijn de basisprincipes van informatiebeveiliging, welke maatregelen moeten minimaal getroffen worden om aan de zorgplicht te voldoen, hoe wordt een risicoanalyse uitgevoerd en waar moet op gelet worden bij het nemen van maatregelen om informatie te beveiligen? Ook is er aandacht voor het organiseren van cyberhygiëne in de organisatie, zodat medewerkers bewust zijn van cyberveiligheid.

8. Incidenten en datalekken

Indien er sprake is van een datalek, oftewel van een inbreuk op de beveiliging in verband met persoonsgegevens moet de verwerkingsverantwoordelijke dit binnen 72 uur melden bij de toezichthouder, tenzij het niet waarschijnlijk is dat het datalek een risico oplevert voor de betrokkenen. Als het datalek waarschijnlijk een risico oplevert voor de betrokkenen, moeten ook zij zo snel mogelijk worden geïnformeerd. Organisaties moeten hierop voorbereid zijn.

De wetgever en de toezichthouders verwachten dat verwerkers van persoonsgegevens onverwijld datalekken doorgeven aan verwerkingsverantwoordelijken. Om dit mogelijk te maken zijn er verwerkersovereenkomsten nodig waarin duidelijke afspraken over procedures en processen zijn gemaakt. De verwerkingsverantwoordelijke en verwerker ondersteunen de processen rond datalekken met een managementsysteem.

Het voorbereid zijn op incidenten en datalekken bestaat uit het organiseren van het signaleren, vastleggen en afhandelen van datalekken, inclusief het melden van datalekken bij de toezichthouder en bij de betrokkenen. Er zijn verschillende rollen bij betrokken die verantwoordelijk zijn voor verschillende taken en gezamenlijk een datalekteam kunnen vormen.

De FG ziet erop toe dat het voorbereid zijn op datalekken adequaat plaatsvindt en adviseert de organisatie bij het afhandelen van datalekken en bij het melden bij de toezichthouder en bij de betrokkenen. Welke stappen moeten hierbij worden doorlopen en welke besluiten moeten worden genomen? Welke rol speelt de FG? En wat als nu er toch een sanctie dreigt te worden opgelegd?

In deze cursus worden aan de hand van praktijkvoorbeelden de stappen doorlopen die genomen moeten worden ter voorbereiding op en bij de afhandeling van datalekken.

C Organiseren van bedrijfsactiviteiten

9. Kennis en veranderen

Om te voldoen aan de AVG en ook aan andere wetgeving die de bescherming van privacy en persoonsgegevens raakt, is kennis bij het management en de medewerkers onmisbaar. Als kennis en bewustwording ontbreken of niet voldoende aanwezig zijn in de organisatie, zal iedere andere stap om meer volwassen te worden op het gebied van privacy en gegevensbescherming niet gaan slagen.

Om kennis en bewustwording bij het management en de medewerkers te organiseren is kennismanagement noodzakelijk. Wet- en regelgeving ontwikkelt voortdurend en de verschillende rollen en verantwoordelijkheden van medewerkers zorgen voor verschillende niveaus van kennisbehoefte en ook voor verschillende manieren van kennisoverdracht.

Om privacy en gegevensbescherming daadwerkelijk te verankeren in een organisatie is naast kennis van privacywetgeving en informatiebeveiliging ook gedragsverandering van medewerkers nodig. Als FG wil je dat bestuurders, managers en medewerkers niet alleen voldoen aan regels, maar ook écht anders gaan denken en handelen. Om een organisatie te laten bewegen moet een FG over kennis en vaardigheden beschikken om gedrag van de organisatie en haar medewerkers positief te kunnen beïnvloeden.

In deze cursus krijgt de FG handvaten om kennismanagement toe te passen in de eigen organisatie, waarbij aandacht is voor de verschillende rollen en verantwoordelijkheden van management en medewerkers. Ook doet de FG kennis op van verandermanagement en gedragsbeïnvloeding. Uiteindelijk leidt kennisopbouw, bewustwording en gedragsveranderingen tot het bestendigen van privacy en gegevensbescherming in een organisatie.

10. Integreren van gegevensbescherming in bedrijfsactiviteiten

Het organiseren van bedrijfsactiviteiten met behulp van bedrijfsprocessen waarin beheers- en beveiligingsmaatregelen “by design” zijn opgenomen is noodzakelijk voor het effectief beschermen van persoonsgegevens. Om gegevensbescherming te integreren in de bedrijfsactiviteiten is overzicht en inzicht nodig van alle verwerkingen waarvoor een

organisatie verantwoordelijk is. Zo wordt duidelijk welke verwerkingen bij welke bedrijfsactiviteiten plaatsvinden en kan het verantwoordelijkheids- en aansprakelijkheidsdomein worden bepaald.

Nog te vaak zien we dat bij bepaalde bedrijfsactiviteiten nauwelijks of onvoldoende rekening wordt gehouden met privacy en gegevensbescherming. Dat zien we bijvoorbeeld bij de afdeling inkoop, waar in contracten met ICT-dienstverleners onvoldoende rekening wordt gehouden met de AVG en bij de afdeling HR, niet alleen als het gaat om arbeidscontracten maar ook in geval van ziekteverzuim en in registraties van functioneren en ontwikkeling van medewerkers.

In deze cursus wordt aandacht gegeven aan de bedrijfsactiviteiten Inkoop, Verkoop en HR in relatie tot het integreren van beveiligingsmaatregelen ”by design” zodat persoonsgegevens effectief beschermd worden. Aan de hand van praktijkvoorbeelden wordt duidelijk welke aanpassingen nodig zijn om te voldoen aan wettelijke verplichtingen.

D Assessment en audit

11. Organiseren van accountability (verantwoording)

De bedrijfsleiding moet verantwoorden afleggen over het effectief beschermen van persoonsgegevens, zo schrijft de AVG voor. De bedrijfsleiding verantwoordt zich achteraf over het effectief beschermen van persoonsgegevens voor een bepaalde periode. Een dergelijke verantwoording kan alleen als de bedrijfsleiding beschikt over voldoende systematisch verzameld en vastgelegd bewijs dat de getroffen beheers-, beveiligings-, en compliance maatregelen passend zijn en dat de persoonsgegevens effectief zijn beschermd.

De bedrijfsleiding zet haar verantwoording kracht bij door het hanteren van een verantwoordingsproces dat aansluit bij andere verantwoordingsprocessen, bijvoorbeeld de maatschappelijke en fiscale verantwoording. Sluitstuk van dit proces is de bevestiging van een onafhankelijke professional die de verantwoording bevestigt of er een – goedkeurende – verklaring/ mededeling bij afgeeft.

De wetgever voorziet in een dergelijk proces met een gedragscode. Wij behandelen in deze cursus een verantwoordingsproces gericht op het voldoen aan de verantwoordingsplicht uit artikel 5, tweede lid van de AVG. Ook behandelen we het belang van een privacy en security administratie, onmisbaar om te voldoen aan de verantwoordingspicht.

12. DPIA, DTIA en DLIA: praktische toepassing

Een Data Protection Impact Assessement (DPIA) wordt uitgevoerd als een verwerking waarschijnlijk een hoog risico inhoudt voor het uitoefenen van de rechten en vrijheden van natuurlijke personen. De aanleiding kan zijn de introductie van nieuwe beheers-, beveiligings-,

en compliance-maatregelen of ondersteunende IT-systemen. De FG heeft een adviserende rol bij het uitvoeren van een DPIA.

Als persoonsgegevens buiten de EU worden gedeeld, kunnen de rechten van betrokkenen mogelijk geschaad worden als niet vastgesteld is dat de partij buiten de EU de persoonsgegevens goed beschermt. De EU heeft de wetgeving van diverse landen buiten de EU beoordeeld als gelijkwaardig als de AVG en voor deze landen is een adequaatheidsbesluit afgegeven.

Voor de landen waarvoor het adequaatheidsbesluit niet geldt, zal middels een Data Transfer Impact Assessment (DTIA) per geval moeten vaststellen of de wetgeving of de rechtspraktijk van het derde land al of niet afbreuk doet aan de passende bescherming van persoonsgegevens en of aanvullende maatregelen nodig zijn. Een DTIA moet worden uitgevoerd door de partij die de persoonsgegevens doorgeeft aan een partij in het derde land. Deze organisatie kan zowel een verwerkingsverantwoordelijke als een verwerker zijn. Ook bij het uitvoeren van een DTIA is de FG nauw betrokken.

Met een Data Legal Impact Assessment (DLIA) kan vastgesteld worden of er kosten- en aansprakelijkheidsrisico's zijn omdat niet wordt voldaan aan wettelijke verplichtingen of omdat er geen goede contractuele afspraken zijn gemaakt met andere partijen. Een DLIA kent dezelfde aanpak als een DPIA en een DTIA en ook hierbij is de FG betrokken als het gaat om rechten en verplichtingen op het gebied van privacy en gegevensbescherming.

In deze cursus wordt ingegaan op vragen als: in welke situaties moet een DPIA, DTIA of een DLIA worden uitgevoerd, hoe wordt een DPIA, DTIA of een DLIA uitgevoerd, hoe kun je als FG toezicht houden op de uitvoering ervan en hoe kun je de resultaten beoordelen.

Totaalaantal cursussen	12
Zelfstudie	192
Deelname workshops (op locatie of online)	48
Totaal aantal uren studiebelasting	***240***

Voor wie?

De Opleiding is geschikt voor (aankomende) FG's, privacy professionals, compliance officers en iedereen die verantwoordelijk is voor gegevensbescherming en privacy binnen de organisatie.

Organisatie van de opleiding

Deelnemers aan de Opleiding FG krijgen toegang tot een persoonlijke leeromgeving. In deze leeromgeving is voor elke cursus van de opleiding de theorie en achtergrondinformatie te vinden. Elke cursus kent een workshop waarin de theorie nader wordt toegelicht, praktijkvoorbeelden worden besproken en waarin alle ruimte is voor het stellen van vragen.

Iedere cursus wordt afgesloten met een toets. Onderdeel van de opleiding is de examentraining voor de kennistoets van het NRFG.

Investering

Geïnteresseerden die zich graag willen laten bijscholen op één of meer onderdelen van deze leergang zijn van harte welkom om één of meer cursussen van deze opleiding te volgen. Een afzonderlijke cursus kost €500, (exclusief BTW). De opleiding FG kost € 5.500, - (exclusief BTW). Particulieren en overheidsinstellingen zijn vrijgesteld van BTW.

Inschrijven

Duthler Academy

Kennis, groei & verandering

Onze medewerkers staan klaar om uw vragen te beantwoorden. U kunt telefonisch contact opnemen. U kunt uiteraard ook een e-mail sturen.

Hoofdkantoor:

Frankenslag 137

2582 HH Den Haag

+31 (0) 70 392 22 09

servicedesk@duthleracademy.nl

https://duthleracademy.nl/