Onderwijs- en examenregeling Leergang FG

2018 en verder*

Auteur: mr. P.L. Coté MBA, mr. J.A. Duthler
Datum: 13 september 2018
Status: concept
Versie: 0.1
Docname: 180913a oer Leergang FG_2018 ev

*NB Deze oer geldt voor de deelnemers die zich op of na 1 oktober 2018 hebben ingeschreven voor de Leergang FG.

Inhoud

Inleiding

Duthler Academy

De Leergang FG wordt aangeboden door de Duthler Academy, onderdeel van Duthler Associates adviesbureau voor recht, bestuur en ICT.

Geheimhouding

Deelnemers moeten zaken die ingebracht worden door andere deelnemers geheimhouden. Bijvoorbeeld privacygevoelige zaken die aan de orde komen tijdens de workshops.

Volgorde

Afgezien van de modules A1 en A2 die als eerste gevolgd moeten worden, geldt er geen volgorde voor het volgen van modules.

Registerinschrijving

Na het succesvol afleggen van de tentamens van alle 30 modulen ontvangt de afgestudeerde het certificaat “Functionaris voor gegevensbescherming” van de Duthler Academy en wordt hij of zij desgewenst opgenomen in het FG-register. Door deel te nemen aan de bijeenkomsten van een privacy kennisgroep van Duthler Associates, behaalt de FG de jaarlijks vereiste Permanente Educatie-punten die vereist zijn voor handhaving van de registerinschrijving.

Indien een deelnemer niet alle modulen van de leergang FG wil volgen ontvangt hij na het succesvol afleggen van tentamens een certificaat waarin staat vermeld voor welke modulen hij succesvol een tentamen heeft afgelegd.

Na het succesvol afleggen van de tentamens van de eerste drie modulen (A1a, A1b en A1c) kan een deelnemer als aspirant FG desgewenst worden opgenomen in het FG Register.

De onderwijs- en examenregeling

Bij het opstellen van een onderwijs- en examenregeling (oer) voor de Leergang FG zijn de bepalingen uit de Wet op het hoger onderwijs en wetenschappelijk onderzoek zoveel mogelijk gevolgd. Voor dit uitgangspunt is gekozen, omdat de Leergang FG van postacademisch niveau is en voor wat betreft het niveau als een opleiding in de zin van de Whw beschouwd kan worden. Voor de goede orde volgt hieronder de tekst van artikel 7.13 Whw.

Onderwijs- en examenregeling

1. Het instellingsbestuur stelt voor elke door de instelling aangeboden opleiding een onderwijs- en examenregeling vast. De onderwijs- en examenregeling bevat adequate en heldere informatie over de opleiding of groep van opleidingen.
2. In de onderwijs- en examenregeling wordt, per opleiding of groep van opleidingen de geldende procedures en rechten en plichten vastgelegd met betrekking tot het onderwijs en de examens.

Daaronder worden ten minste begrepen:

a. de inhoud van de opleiding en van de daaraan verbonden examens,
a1. de wijze waarop het onderwijs in de desbetreffende opleiding wordt geëvalueerd,
b. de inhoud van de afstudeerrichtingen binnen een opleiding,
c. de kwaliteiten op het gebied van kennis, inzicht en vaardigheden die een student zich bij beëindiging van de opleiding moet hebben verworven,
d. waar nodig, de inrichting van praktische oefeningen,
e. de studielast van de opleiding en van elk van de daarvan deel uitmakende onderwijseenheden,
f. de nadere regels, bedoeld in de artikelen 7.8b, zesde lid, en 7.9, vijfde lid, (nvt op LGFG)
g. ten aanzien van welke masteropleidingen toepassing is gegeven aan artikel 7.4a, achtste lid, (nvt op LGFG)
h. het aantal en de volgtijdelijkheid van de tentamens alsmede de momenten waarop deze afgelegd kunnen worden,
i. de voltijdse, deeltijdse of duale inrichting van de opleiding,
j. waar nodig, de volgorde waarin, de tijdvakken waarbinnen en het aantal malen per studiejaar dat de gelegenheid wordt geboden tot het afleggen van de tentamens en examens,
k. de nadere regels bedoeld in artikel 7.10, vierde lid,Whw (nvt op LGFG)
l. of de tentamens mondeling, schriftelijk of op een andere wijze worden afgelegd, behoudens de bevoegdheid van de examencommissie in bijzondere gevallen anders te bepalen,
m. de wijze waarop studenten met een handicap of chronische ziekte redelijkerwijs in de gelegenheid worden gesteld de tentamens af te leggen,
n. de openbaarheid van mondeling af te nemen tentamens, behoudens de bevoegdheid van de examencommissie in bijzondere gevallen anders te bepalen,
o. de termijn waarbinnen de uitslag van een tentamen bekend wordt gemaakt alsmede of en op welke wijze van deze termijn kan worden afgeweken,
p. de wijze waarop en de termijn gedurende welke degene die een schriftelijk tentamen heeft afgelegd, inzage verkrijgt in zijn beoordeelde werk,
q. de wijze waarop en de termijn gedurende welke kennis genomen kan worden van vragen en opdrachten, gesteld of gegeven in het kader van een schriftelijk afgenomen tentamen en van de normen aan de hand waarvan de beoordeling heeft plaatsgevonden,

r. de gronden waarop de examencommissie voor eerder met goed gevolg afgelegde tentamens of examens in het hoger onderwijs, dan wel voor buiten het hoger onderwijs opgedane kennis of vaardigheden, vrijstelling kan verlenen van het afleggen van een of meer tentamens,
s. waar nodig, dat het met goed gevolg afgelegd hebben van tentamens voorwaarde is voor de toelating tot het afleggen van andere tentamens,
t. waar nodig, de verplichting tot het deelnemen aan praktische oefeningen met het oog op de toelating tot het afleggen van het desbetreffende tentamen, behoudens de bevoegdheid van de examencommissie vrijstelling van die verplichting te verlenen, al dan niet onder oplegging van vervangende eisen,
u. de bewaking van studievoortgang en de individuele studiebegeleiding,
v. indien van toepassing: de wijze waarop de selectie van studenten voor een speciaal traject binnen een opleiding, bedoeld in artikel 7.9b, plaatsvindt, (nvt op LGFG)
x. de feitelijke vormgeving van het onderwijs, en
y. indien van toepassing: de regeling, bedoeld in artikel 7.9a, derde lid, tweede volzin. (nvt op LGFG)

Deze onderwerpen worden hieronder besproken, voor zover ze van toepassing zijn op de Leergang FG.

2.1 de inhoud van de opleiding en examens

2.1.1 Algemeen

a. Een module bestaat uit één tot vier dagdelen cursus die gegeven wordt bij de Duthler Academy door privacy professionals van Duthler Associates en deskundige gastdocenten. Tijdens de cursus worden aan de stof gerelateerde praktijkcasus behandeld. Daarnaast wordt van de deelnemer verwacht dat hij of zij de verplichte literatuur bestudeert die online aangeboden wordt. Uiteraard is er ruimte voor praktijkgerichte vragen. Hierna wordt de module (per dagdeel) afgesloten met een tentamen.

2.1.2 Examencommissie

a. Er is een examencommissie voor de opleiding. De examencommissie is een onafhankelijk orgaan en bestaat uit 3 door het instellingsbestuur te benoemen leden.
b. De examencommissie stelt op objectieve en deskundige wijze vast of een cursist voldoet aan de voorwaarden die de onderwijs- en examenregeling stelt ten aanzien van kennis, inzicht en vaardigheden die nodig zijn voor het verkrijgen van het certificaat.
c. De examencommissie heeft de volgende taken en bevoegdheden:

- het borgen van de kwaliteit van de tentamens;

- het vaststellen van richtlijnen en aanwijzingen binnen het kader van de onderwijs- en examenregeling om de uitslag van tentamens te beoordelen en vast te stellen;

- het verlenen van vrijstelling voor het afleggen van één of meer tentamens;
- het aanwijzen van de examinatoren.

d. De examencommissie kan regels vaststellen over de uitvoering van haar taken en bevoegdheden.
e. De examencommissie kan onder door haar te stellen voorwaarden bepalen dat niet ieder tentamen met goed gevolg afgelegd hoeft te zijn om vast te stellen dat het certificaat kan worden uitgereikt (compensatieregeling).
f. Bij de samenstelling van de examencommissie wordt rekening gehouden met inhoudelijke deskundigheid op het gebied van wet- en regelgeving inzake privacy en gegevensbescherming, organisatie, ICT, AO/IB en beveiliging.
g. Het instellingsbestuur wijst één van de leden aan als voorzitter. Bij staking van stemmen over besluiten geeft diens stem de doorslag.
h. De examencommissie neemt rechtsgeldige besluiten indien tenminste twee leden, waaronder de voorzitter, aanwezig zijn.
i. Het secretariaat van de examencommissie wordt gevoerd door de office manager van Duthler Associates.

2.1.3 de wijze waarop het onderwijs wordt geëvalueerd

Het onderwijs wordt geëvalueerd door middel van zelfevaluatie door de leiding van de opleiding. Daarbij wordt de feedback van deelnemers betrokken en de evaluatieformulieren die de deelnemers na een onderwijsactiviteit invullen. De opleiding wordt ook geëvalueerd door diverse externe instanties waaronder NRTO en Cedeo.

2.2 inhoud van de afstudeerrichtingen

a. De leergang FG kent één afstudeerrichting: Functionaris voor Gegevensbescherming.

2.3 competenties

a. Competenties: de kwaliteiten op het gebied van kennis, inzicht en vaardigheden die een student zich bij beëindiging van de opleiding moet hebben verworven. Het goed uitvoeren van de taken van de FG vergt kennis en vaardigheden. De kennis die benodigd is, is zowel breed als diep en betreft onder andere de volgende onderwerpen, zowel op strategisch als op uitvoerend niveau:

- Juridisch: o.a. kennis van algemene en sectorspecifieke wet- en regelgeving
- Bestuurlijk: o.a. governance en compliance
- Organisatorisch: o.a. administratieve organisatie, beheercycli en procedures
- Technisch: o.a. privacy enhancing technologies en informatiebeveiliging

b. Daarnaast zijn goede communicatieve vaardigheden onontbeerlijk. Niet alleen onderhoudt de FG contact met interne stakeholders als de Raad van Bestuur, de Raad van Toezicht en uitvoerende professionals, maar ook is hij aanspreekpunt voor de toezichthouder én de betrokkene over alle aangelegenheden die verband houden met de verwerking van de persoonsgegevens van de betrokkene.

c. De FG moet bovendien voldoende draagvlak creëren en gezag hebben om de functie goed uit te oefenen. De FG moet stevig in zijn schoenen staan: als onafhankelijk toezichthouder komt de FG regelmatig in de positie dat hij/zij constateert dat bestaande handelswijzen of situaties niet zijn toegestaan. Dit vereist kennis van organisaties (hoe werken organisaties, ‘dark sides’ van organisaties en personen) en kennis van de organisatie waar het om gaat (hoe werkt deze organisatie, waar zitten risico’s?)

2.4 inrichting van praktische oefeningen

a. De Leergang FG kent geen stageverplichting. De praktijkcomponent komt in de Leergang FG aan bod door de behandeling van praktijkcases in de cursus.

2.5 studielast van de opleiding en van de onderwijseenheden

De studiebelasting van de Leergang FG bedraagt 20 uur voor een module die bestaat uit een dagdeel:

- 4 uur deelname cursus op locatie Frankenslag en 16 uur zelfstudie.
- De studiebelasting van een module die uit twee dagdelen bestaat bedraagt 40 uur, twee keer 4 uur deelname cursus op locatie Frankenslag en 32 uur zelfstudie.
- De studiebelasting van een module die uit drie dagdelen bestaat bedraagt 60 uur, drie keer 4 uur deelname cursus op locatie Frankenslag en 48 uur zelfstudie.
- De studiebelasting voor de gehele Leergang FG bestaat uit 30 modules verdeeld over 30 dagdelen. De totale studiebelasting van de Leergang FG bedraagt daarmee 600 uur.

2.6 bindend studieadvies

a. De regeling rond het bindend studieadvies zoals bedoeld in de Wet op het hoger onderwijs en wetenschappelijk onderzoek is niet van toepassing op de Leergang FG.

2.7 het aantal en de volgtijdelijkheid van de tentamens

a. Elk dagdeel van een module wordt afgesloten met een tentamen. De tentamens voor de modules A1 en A2 moeten met goed gevolg zijn afgelegd voordat andere tentamens kunnen worden afgelegd.

2.8 voltijdse, deeltijdse of duale inrichting van de opleiding

a. De opleiding wordt in deeltijdvorm aangeboden en kan naar behoefte opgesteld worden.

2.9 Tentamens

a. Een tentamen kan per jaar vier maal worden afgelegd.
b. De geldigheidsduur van met goed gevolg afgelegde toetsen bedraagt 4 jaar. De examencommissie is bevoegd om de geldigheidsduur te verlengen.
c. De tentamens worden schriftelijk (digitaal) afgelegd, behoudens de bevoegdheid van de examencommissie om in bijzondere gevallen anders te bepalen.
d. De examencommissie beslist in individuele gevallen hoe een student ingeval van handicap of chronische ziekte redelijkerwijs in de gelegenheid wordt gesteld de tentamens af te leggen.
e. Mondelinge tentamens zijn niet openbaar behoudens de bevoegdheid van de examencommissie in bijzondere gevallen anders te bepalen.

2.10 termijn waarbinnen de uitslag van een tentamen bekend wordt gemaakt

a. De tentamenuitslag wordt binnen zes weken na de uiterste inleverdatum van het tentamen aan de student meegedeeld. Wanneer deze termijn overschreden dreigt te worden deelt de examencommissie binnen deze termijn aan de student mee wanneer de tentamenuitslag aan de student wordt meegedeeld.

2.11 inzage

a. De student die een schriftelijk (digitaal) tentamen heeft afgelegd, kan op verzoek, inzage krijgen in zijn beoordeelde werk binnen vier weken nadat de tentamenuitslag aan hem is meegedeeld. De inzage vindt plaats bij de Duthler Academy. In aanwezigheid van de examinator krijgt de student inzage in zijn beoordeelde werk.

2.12 kennisneming van vragen en opdrachten

a. De student die een schriftelijk (digitaal) tentamen heeft afgelegd, kan binnen vier weken nadat de tentamenuitslag aan hem is meegedeeld, kennisnemen van vragen en

opdrachten van een schriftelijk (digitaal) afgenomen tentamen en van de normen aan de hand waarvan de beoordeling heeft plaatsgevonden. De kennisname vindt plaats bij de Duthler Academy in aanwezigheid van de examinator.

2.13 vrijstelling

a. De examencommissie kan voor eerder met goed gevolg afgelegde tentamens of examens in het hoger onderwijs, dan wel voor buiten het hoger onderwijs opgedane kennis of vaardigheden, vrijstelling verlenen voor het afleggen van een of meer tentamens.

2.14 voorwaarde voor de toelating tot het afleggen van tentamens

a. De tentamens kunnen worden gemaakt na het volgen van het dagdeel cursus op locatie Frankenslag te Den Haag. De tentamens voor de modules A1 en A2 moeten met goed gevolg zijn afgelegd voordat andere tentamens kunnen worden afgelegd.

2.15 verplichting tot het deelnemen aan praktische oefeningen

a. De Leergang FG kent geen stageverplichting. De praktijk component komt in de Leergang FG aan bod door de behandeling van praktijkcases.

2.16 bewaking van studievoortgang

a. Duthler Academy bewaakt de studievoortgang door middel van de registratie van de toetsresultaten.

Toelichting op de modules van de Leergang FG

A. Formeel – Juridisch

Om als FG te kunnen functioneren, is multidisciplinaire kennis nodig. Kennis op het gebied van wet- en regelgeving, organisatie, ICT, AO/IB en beveiliging. Om zijn advies- en toezichtstaken goed te kunnen uitvoeren moet de FG over genoemde multidisciplinaire kennis beschikken. Zonder gedegen kennis van privacywetgeving is het dan ook onmogelijk goed als FG te functioneren. In cluster A wordt een viertal cursussen aangeboden gericht op de juridische kennisvergaring. Met de verworven kennis is de FG in staat de Wbp, Avg en aanpalende wet- en regelgeving te interpreteren en zijn functie deugdelijk te vervullen.

A1 De inleiding omtrent privacy

Doel Na deze cursus kennen deelnemers de basisbegrippen van privacywetgeving, de uitgangspunten, de verschillende (privacy)rollen in een organisatie en de belangrijkste rechten en verplichtingen. Ook kennen deelnemers de hoofdlijnen en begrippen van de belangrijkste wet- en regelgeving op het gebied van netwerk informatiebeveiliging, elektronische vertrouwensdiensten en identitymanagement.

Duur Drie dagdelen

A1a Overzicht van de huidige privacywetgeving

De huidige wetgeving op het vlak van gegevensbescherming en privacy wordt bepaald door de Europese privacyrichtlijn 95/46/EG en de implementatie hiervan in nationale wetgeving van EU-lidstaten. In Nederland spreken wij over de Wet bescherming persoonsgegevens (Wbp). In deze module leren de deelnemers de basisbegrippen van de huidige privacywetgeving, de uitgangspunten, de verschillende (privacy)rollen in een organisatie, de belangrijkste rechten en verplichtingen van de Wbp.

A1b De Avg, de nieuwe privacyregels

De Europese Algemene verordening gegevensbescherming (Avg) is in werking getreden en zal van toepassing worden op 25 mei 2018. Deze verordening staat in module A1b centraal. De uitgangspunten, de begrippen, de verschillende (privacy)rollen in een organisatie, de belangrijkste rechten en verplichtingen worden behandeld. Na het volgen

van de module kan de kandidaat een inschatting maken van de te treffen maatregelen van deze wet- en regelgeving in de eigen organisatie.

A1c Overzicht in wetgeving rond beveiliging en identitymanagement

Een belangrijk aandachtspunt van gegevensbescherming en het borgen van de privacy is het organiseren van informatiebeveiliging. Los hiervan worden meer en meer regels vanuit het perspectief van informatiebeveiliging en identitymanagement opgelegd, zoals de Europese richtlijn Netwerk informatiebescherming (NIB). Na het volgen van deze module heeft de kandidaat een overzicht van wat er formeel juridisch op het vlak van informatiebeveiliging en identitymanagement speelt. En hoe dat samenhangt met de wetgeving op het vlak van gegevensbescherming en privacy.

A2 De e-privacyverordening

Doel Na deze module hebben deelnemers inzicht in de e-privacyverordening en kennen ze de samenhang met de Avg. Deelnemers kunnen zich een beeld vormen van de veranderingen die de verordening met zich meebrengt en de betekenis daarvan. Ook hebben zij inzicht in de betekenis daarvan voor hun toezichts- en adviestaken.

Duur Een dagdeel

A3 De Avg in internationaal perspectief

Doel Gegevensverwerkingen die plaatsvinden buiten de EU en betrokkenen betreffen die gevestigd zijn in de EU, zijn aan strenge regels gebonden. Na deze cursus kennen deelnemers de voorwaarden waaraan doorgifte van persoonsgegevens naar derde landen en/of internationaal opererende organisaties moet voldoen.

Duur Twee dagdelen

A3a De Avg in een internationaal perspectief: Europa

In deze module maken we kennis met de Europese aspecten van de privacywetgeving. De Avg is het voorlopig sluitstuk van een ontwikkeling in de Europese gegevensbescherming. Aan de hand van onderwerpen als 'afstemming', 'toezicht', 'uitwisseling tussen lidstaten' volgen we het spoor terug. We zullen dergelijke onderwerpen uit de Avg ook tegenkomen in Verdragen als het Europees Verdrag voor de rechten van de mens uit 1950 en het Verdrag van Straatsburg van 1981. Een belangrijk onderdeel van deze module "Europese aspecten" is gewijd aan de samenhang en het onderscheid tussen het Verdrag van Straatsburg, afkomstig van de Raad van Europa en de regelgeving van de EU zoals de Richtlijn en de Avg. In de workshop wordt nader ingegaan op de verhouding tussen beide stelsels. In de module komt verder aan de orde hoe het toezicht op Europees niveau is

geregeld en hoe dit veranderd als gevolg van de Avg. De samenwerking tussen de nationale toezichthouders in de Artikel 29 Werkgroep zal worden toegelicht. Verder worden de beroepsgang naar het Europese Hof van Justitie en het Europese Hof voor de Rechten van de Mens behandeld aan de hand van enkele recente uitspraken.

A3b De Avg in een internationaal perspectief: V.S., verre oosten en rest van de wereld

In deze module, die samen met First Lawyers is opgesteld, zal worden stilgestaan bij de globalisering van de gegevensverwerking. De module heeft ten minste drie doelstellingen. In de eerste plaats wordt uw kennis van de Europese randvoorwaarden die gelden op de internationale gegevensuitwisseling vergroot. In de tweede plaats zal u kennismaken met de risico's van globalisering. Er zal worden ingezoomd op vier privacyregimes, te weten: V.S., Japan, India en Australië. In de laatste plaats gaat u op zoek naar oplossingen van voornoemde risico's van globalisering.

A4 Privacy en aanpalende wetgeving

Doel Na deze cursus hebben de deelnemers inzicht in de wet- en regelgeving die in relatie staat tot de Wbp of Avg. Dit is zowel wet- en regelgeving die een nadere invulling betreft van de formele wetgeving, als sectorspecifieke of onderwerp specifieke wet- en regelgeving, als aanpalende wet- en regelgeving. Voorbeelden van de eerste categorie zijn besluiten en ministeriële regelingen. Voorbeelden van de tweede categorie zijn formele wetten als de Wet geneeskundige behandelovereenkomst (Wgbo), de Wet Basisregistratie Personen (BRP) en de Wet politiegegevens (Wpg). Voorbeelden van de derde categorie betreffen boek 2 van het BW waarin het jaarrekeningenrecht wordt geregeld en governancecodes. Bijzondere aandacht wordt geschonken aan de gegevensbeschermingsregels in het HR-domein.

Duur Een dagdeel

B. Governance en Compliance

Indien de formeel - juridische kennisbasis is gelegd (zoals aangeboden in cluster A) kan de governance & compliance vorm worden gegeven. Hierbij is het primaire doel het voorkomen van een sanctie van materieel belang. Secundair kunnen ook andere overwegingen een rol spelen. Wij kunnen denken aan het beperken van bestuurdersaansprakelijkheid, verhogen van datakwaliteit en of het beter kennen van bijvoorbeeld cliënten, studenten, burgers en of medewerkers. Als gevolg van de formeel-juridische regels omtrent verwerkingen van (persoons)gegevens “schuiven” taken, bevoegdheden en verantwoordelijkheden in bestaande bestuurlijke kaders. Organisaties, met enige omvang en of die verantwoordelijk zijn voor het verwerken van bijzondere persoonsgegevens op enige schaal, zullen een functionaris voor de gegevensbescherming (FG) (moeten) aanstellen. Binnen het bestuurlijke kader wordt de FG in de buurt van de raad van commissarissen / toezicht op passende afstand gepositioneerd. Hiernaast vervult de FG operationele taken of ziet daarop toe. De formeel juridische status van de FG is van een andere orde dan die van een functionaris information security officer (ISO), een adviseur administratieve organisatie (AO/IT) en een bedrijfsjurist (JUR). Het is vanuit een oogpunt van good governance belangrijk dat de taken, bevoegdheden en verantwoordelijkheden van de FG duidelijk en transparant zijn. Na het volgen van cluster B moet de cursist in staat zijn vanuit het perspectief van gegevensverwerking de governance & compliance voor de eigen organisatie vorm te geven. En binnen die context de taken, bevoegdheden en verantwoordelijkheden van de FG te benoemen.

Een belangrijk graadmeter in hoeverre een organisatie de governance & compliance op orde heeft is de mate waarin een verantwoordelijke er in slaagt datalekken te vermijden, detecteren en melden bij de toezichthouder. Het organiseren van het voorkomen van en opvangen wanneer er onverhoopt toch datalekken worden geconstateerd, het aan sleutelfunctionarissen toedelen van taken, bevoegdheden en verantwoordelijkheden en doortastend optreden op het moment dat de toezichthouder sancties oplegt vormt een belangrijk onderdeel van de module.

B1. De FG: positie, taken, bevoegdheden en verantwoordelijkheden

Doel In de Avg worden de aanwijzing van de FG, zijn positie in de organisatie en zijn taken en bevoegdheden nader geregeld. In vergelijking met de Wbp kunnen we zeggen dat de Avg de functie van de FG nader inkleurt. Na deze module kennen deelnemers de belangrijkste eisen die de Wbp en Avg stellen aan de positie van de FG en zijn taken, bevoegdheden en verantwoordelijkheden. Ook hebben de deelnemers inzicht in de belangrijkste verschillen met de Wbp. Deelnemers krijgen tevens handvatten aangereikt voor de nadere invulling van hun functie en positie.

Duur Een dagdeel

B2. De Avg en privacybeleid, policyframework en baseline

Doel De FG heeft tot taak toe te zien op de naleving van het privacybeleid. Aan het privacybeleid ligt het formeel-juridisch kader ten grondslag. Het formeel-juridisch kader wordt niet alleen bepaald door de Avg, maar ook door de aanpalende wet- en regelgeving. Met een policyframework worden deze wet- en regelgeving met elkaar in verband gebracht. De te treffen maatregelen en procedures worden hiervan afgeleid en in een baseline vastgelegd. Na deze cursus kennen deelnemers de eisen die de Avg stelt aan privacybeleid, de rol van de FG en de ISO en zijn zij in staat het privacybeleid voor hun organisatie te ontwikkelen danwel te beoordelen. Ook zijn de deelnemers in staat een policyframework en –baseline te ontwikkelen dan wel te beoordelen. Deze modules worden afgesloten met het schrijven van een privacybeleid.

Duur Twee dagdelen

B2a Privacybeleid: Policyframework, normenkader en privacyorganisatie

De grote diversiteit aan regelgeving maakt het noodzakelijk om binnen een organisatie beleid op te stellen. In dit beleid zullen de nationale, internationale, sectorale, aanpalende wet- en regeling etc. samengebracht moeten worden tot één werkbare methode voor de praktijk. Met een Policy Framework (gericht op privacy) worden deze wet- en regelgeving met elkaar in verband gebracht. De te treffen maatregelen en procedures worden hiervan afgeleid en in een Normenkader vastgelegd.

B2b Intern en extern privacybeleid

Privacybeleid is op twee fronten van belang. Ten eerste binnen de eigen organisatie. Hoe gaan we met gegevens om en welke gegevens verzamelen we? Ten tweede de informatie voorziening naar de buitenwereld toe. Op beide fronten moet een privacybeleid ontwikkeld worden. Na deze module kan de cursist privacybeleid opstellen.

B3. Governance en compliance

Doel Belangrijke uitgangspunten van de Avg zijn accountability en auditability. Naleving van de Avg zal onderdeel worden van governancecodes en jaarlijkse audits. Deelnemers aan de module leren de eisen van de Avg te vertalen naar het risicomanagement van hun organisatie, zodat compliance aan de verordening onderdeel van het risicobeheerssysteem wordt. Deelnemers worden in staat gesteld om ”in control” te komen van de gegevensbescherming in de organisatie.

Duur Twee dagdelen

B3a Wetgeving in breder perspectief

Belangrijke uitgangspunten van de Avg zijn Accountability en Auditability. Niet compliant gedrag wordt gesanctioneerd met boetes van materieel belang. Hiermee verschilt de Avg niet met wet- en regelgeving uit niet-EU landen. Het is redelijk te veronderstellen dat naleving van de Avg onderdeel zal worden van governancecodes. Hiermee zal de verantwoordelijke in het jaarverslag over het privacybeleid en de resultaten daarvan in de maatschappelijke verantwoording verslag doen. De accountant belast met de wettelijke controle zal nagaan wat de risico's zijn op een sanctie van materieel belang en vaststellen dat het jaarverslag juist is. Invulling wordt gegeven aan de maatregelen van Administratieve Organisatie en Interne Controle (AO/IC) waarbij een brug wordt geslagen naar het denken van R.W. Starreveld, de grondlegger van AO/IC) naar wat thans van belang is in het kader van gegevensbescherming en privacy.

B3b Governance en Compliance - nader uitgewerkt

Centraal staan de vragen: waar grijpt de wet- en regelgeving in, wat zijn de gevolgen voor de verantwoordelijke en wat zijn passende maatregelen en procedures om de risico's te mitigeren? In deze module wordt toegewerkt naar een governance oplossing, welke is uitgewerkt in een methodologie, misschien wel beter gezegd een gedragscode, waarmee door middel van adequaat administreren en documenteren, ook van bewijs van effectieve werking, iedere verantwoordelijke die zich aan die gedragscode houdt zijn Accountability kan aantonen, daarmee auditable is geworden en op basis waarvan hij verantwoording kan afleggen aan het maatschappelijk verkeer, waaronder betrokkenen, toezichthouders zoals de Autoriteit Persoonsgegevens en vele anderen.

B4. Datalekken, en nu?

Doel Indien er sprake is van een inbreuk op de beveiliging of omzeiling van de beveiliging in verband met persoonsgegevens moet de verantwoordelijke dit zonder vertraging melden bij de toezichthouder. Als er nadelige consequenties zijn te verwachten, dienen ook alle betrokkenen te worden geïnformeerd. De organisatie van de verantwoordelijke moet hierop zijn voorbereid. Dit betekent niet alleen dat de informatiebeveiligingsfunctionaris en de FG van een dergelijke verplichting op de hoogte zijn, maar alle medewerkers moeten op de hoogte kunnen zijn. Zij kunnen immers ook in een organisatie achter een datalek komen of er één veroorzaken. Ook zij moeten dan weten wat zij moeten doen, en het belang daarvan kennen.

Duur Twee dagdelen

B4a Voorbereid zijn op een datalek

Na een korte inleiding over het fenomeen "meldplicht" wordt de blik gericht op de toezichthouder. Welke rol neemt deze in, zowel in het algemeen als specifiek gericht op

datalekken. Vervolgens wordt ingegaan op de voorbereidingen, die een organisatie kan treffen ten aanzien van het voorkomen en afhandelen van een datalek. Nader wordt ingegaan op het bepalen van de verantwoordelijkheid en aansprakelijkheid, de privacyboekhouding, contractmanagement en de privacyorganisatie.

B4b Hoe kan en moet ik handelen na een datalek?

Deelnemers aan deze module kunnen na afloop met gebruikmaking van het verstrekte model een “draaiboek datalekken” voor hun eigen organisatie opstellen. Tevens weten zij op welke wijze zij welk bewijsmateriaal moeten documenteren om aan te kunnen tonen dat de verantwoordelijke aan alle eisen op dit punt van de Avg voldoet en kan voldoen. Het melden van een datalek kan betekenen dat de (on)geschiktheid van de informatiebeveiliging en passant wordt meegenomen bij de beoordeling door de AP of een andere toezichthouder.

C. Materieel: opzet, bestaan en werking van maatregelen en mechanismen

Met formeel – juridische kennis, inzicht in de positie en taken, bevoegdheden en verantwoordelijkheden van de functionaris voor de gegevensbescherming (FG) alsmede het invulling geven aan de uitgangspunten accountability en auditability waarbij governance en compliance een belangrijke rol spelen zal de cursist vervolgens de rechten van betrokkenen en verplichtingen van verantwoordelijken nader moeten concretiseren. Hoe kan aan de rechten en verplichtingen concreet invulling worden gegeven? Wat zijn mogelijke te treffen maatregelen, mechanismes en procedures? Welke rollen zijn er te onderscheiden binnen een (privacy)organisatie?
Hoe positioneer ik het informatiebeveiligingsbeleid en relateer dat aan het privacybeleid alsmede het compliancebeleid? Hoe zorg ik er voor dat persoonsgegevens niet langer worden bewaard dan noodzakelijk voor het doel waarvoor ze worden verwerkt? Wat wordt bedoelt met “lifecycle privacy protection management” en hoe kan ik dat handen en voeten geven? In cluster C worden de Avg en aanpalende privacywetgeving vertaald naar praktische beheersmaatregelen in de organisatie. Handvatten worden aangereikt om de privacyregelgeving te verankeren in de organisatie. En – *en dit is misschien wel de grootste uitdaging* – hoe zorg ik voor een adequate regelkring waarbij de verantwoordelijke accountable en auditable is?

C1. Overzicht & inzicht in de verantwoordelijkheden

Doel De verantwoordelijke moet overzicht en inzicht hebben in al waarvoor hij verantwoordelijk en aansprakelijk is. De Avg verplicht hier zelfs toe. De meldplicht waaraan de verantwoordelijke onverwijld moet voldoen, vereist dat de verantwoordelijke zich goed heeft voorbereid. Dit betekent dat niet alleen de verwerkingen moeten worden gedocumenteerd, maar meer nog dat inzicht gaat ontstaan in processen, informatiesystemen, corporate family, dataopslag, beveiligings- en transportsystemen. Daartoe is het van belang dat de verantwoordelijke een privacy- administratie gaat onderhouden, gesteund met goede processen zodanig dat die administratie door onweerlegbaar bewijs evidence based compliant is gedocumenteerd. Deelnemers krijgen inzicht in het belang van het opzetten en onderhouden van een adequate privacy-administratie om te voldoen aan de documentatieplicht, inzicht te geven in de technische beveiligingsplicht en voorbereid te zijn op de meldplicht.

Duur Een dagdeel

C2. Transparantie en effectueren van rechten van betrokkenen

Doel Deelnemers aan deze module krijgen inzicht in alle afzonderlijke plichten, in het belang van het aantoonbaar kunnen laten zien dat de verantwoordelijk tijdig, juist en volledig aan deze plichten heeft voldaan en hoe hij dat organiseert. Dan gaat het over te treffen maatregelen, procedures en mechanismes om bijvoorbeeld betrokkenen binnen vier weken inzage te geven in hun eigen persoonsgegevens, alsook over de consequenties voor aan te schaffen of te ontwikkelen informatiesystemen om het recht van gegevensoverdraagbaarheid te kunnen honoreren. Maar ook gaat het over alle andere vanuit compliance-audits vastgestelde correcte naleving. Denk hierbij aan het vastleggen van compliance waarbij gebruik is gemaakt van continuous audit tools om aan te kunnen tonen vanuit bewijsvoering dat de verantwoordelijke de wetten naleeft en dus zijn verantwoordelijkheid heeft genomen.

Duur Een dagdeel

C3. Informatiebeveiliging, de basis voor privacybescherming

Doel Deelnemers zijn na deelname aan deze module in staat om de eisen die de Avg stelt aan de beveiliging van persoonsgegevens te vertalen in uitgangspunten voor informatiebeveiligingsbeleid. Ook zijn de deelnemers in staat het privacybeleid en informatiebeveiligingsbeleid aan elkaar te relateren en indien wenselijk met elkaar te integreren. Daarbij wordt vanzelfsprekend een relatie gelegd met informatiebeveiligingsnormen, algemene of sectorspecifieke. Voorbeelden van algemene normen zijn die van de ISO 27001 en 27002 en de Richtsnoeren informatiebeveiliging van het College Bescherming Persoonsgegevens. Voorbeelden van sectorspecifieke zijn die van ZekeRe Zorg 3 of het Normenkader informatiebeveiliging hoger onderwijs.

Duur Twee dagdelen

C3a Informatiebeveiliging, de basis voor privacybescherming

Ter bescherming van persoonsgegevens moeten passende technische en organisatorische maatregelen genomen worden, zo wordt bepaald in de Wbp en de Avg. Wat behelzen deze maatregelen nu precies? Hoe moeten risico's ingeschaald worden zodat ingeschat kan worden welke maatregelen afdoende bescherming bieden.

C3b De techniek achter informatiebeveiliging

Als FG is het van belang kennis te hebben over de techniek achter informatiebeveiliging. De technische kennis van de cursisten zal aangevuld worden. Waardoor basiskennis ontstaat over de gevaren en de bijbehorende oplossingen. Begrippen als antivirus, PEN-tests, beheertoegang, mobile devices en cloud komen aan bod.

C4 Lifecycle privacy protection management

Doel De betrokkene krijg grip op zijn/haar eigen leven, en bedrijven en instellingen zullen met dat fenomeen rekening moeten houden. Stel nu eens voor dat de betrokkene daadwerkelijk beschikt over een eigen omgeving/dossier waarmee de betrokkene zijn/haar persoonsgegevens beheert en gemaakte afspraken deelt met bedrijven, instellingen en andere betrokkene. Hoe ziet dat er dan uit en bestaan er al voorbeelden in de markt? Wat zij de gevolgen voor de infrastructuren van de bedrijven en instellingen die in de B:C markt zitten en welke beheers- en beveiligingsmaatregelen moeten worden genomen om compliant te zijn. In de afgelopen jaren bij het tot stand komen van de Avg is door met name wetenschappers nagedacht over hoe een en ander te organiseren. In deze modules wordt een overzicht gegeven van wat er is en hoever het staat met de toepassingen. Na het volgen van een module moet het kennisniveau van de kandidaat verder worden verhoogd. De kandidaat moet in staat zijn ontwikkelingen op de verschillende aandachtspunten te onderkennen en in een breder perspectief te plaatsen. De deelnemer: de aspirant FG moet in staat zijn het woord te voeren over deze ontwikkelingen.

Duur Vier dagdelen

C4a Lifecycle privacy protection management

De commissie LIBE heeft voorgesteld in de Europese Avg de verplichting van lifecycle data protection management op te nemen. In de uiteindelijke tekst is deze verplichting niet opgenomen. Vanuit de structuur van de Avg is wel de facto het principe overeind gebleven. Wat wordt bedoeld met een dergelijk model? Wat zijn de uitgangspunten en de architecturen? Hoe is een en ander uitgewerkt in modellen voor Attribute Based

Credentials en welke afsprakencomplexen liggen hieraan ten grondslag. In deze module komt aan bod wat bedoeld wordt met een dergelijk model.

C4b Architecturen en uitgangspunten

Uitgangspunten worden gevormd door identitymanagement, schema's, policies en practices die wij kennen van het concept van Public Key Infrastructure (PKI) en de elektronische handtekening. Maar ook de ontwikkelingen die zich voordoen op het vlak van outsourcing en clouddiensten. Vanuit deze kaders kan de verschuiving van het beheerparadigma worden toegepast: de betrokkene is "in control" over zijn of haar eigen persoonsgegevens, en er ontstaan nieuwe schema's en architecturen. In verschillende gremia wordt hiermee geëxperimenteerd. Nu de Avg is aangenomen kunnen de architecturen naar het gewenste volwassenheidsniveau worden getrokken.

Deelnemers aan deze cursus worden de uitgangspunten en architecturen voorgehouden. Architecturen die hebben geleid tot toepassingen worden – voor zover beschikbaar – getoond en besproken.

C4c Modellen voor Attribute Based Credentials

Modellen en hun nadere uitwerking hiervan in informatiesystemen op basis van Attribute Based Credentials zijn door verschillende universiteiten uitgewerkt en gedeeld met het maatschappelijk verkeer. Thans werkt de industrie aan meer vereenvoudigde en vooral praktisch hanteerbare modellen. Deelnemers wordt een overzicht geboden van de (uitgevoerde) initiatieven. Voor zover beschikbaar en openbaar worden initiatieven van de industrie besproken en getoond.

C4d Inregelen van een afsprakencomplex

Het inregelen en beheren van lifecycle data protection management en of andere vormen van privacy by design en privacy by default vraagt om een degelijke formeel-juridische verankering. Als gevolg van de verschuiving in de beheerparadigma moeten afsprakencomplexen opnieuw worden ontworpen, uitgewerkt en verankerd in technologie. Hierbij beschouwen wij zowel het perspectief van de verantwoordelijke als het perspectief van de betrokkene. Het beheer heeft dan ook betrekking op het management van de lifecycle van de credentials. Zoals het veelal gaat zijn er "sunny days" en "rainy days". Als de credentials van de betrokkenen en de verantwoordelijke accorderen kunnen de verwerkingen zonder problemen plaatsvinden. Is er echter sprake van discrepanties en conflicten dan zal er geëscaleerd moeten worden naar een derde partij of wordt de gang naar de toezichthouder of rechter gekozen. Deelnemers aan deze module krijgen inzicht in de achtergronden en de uitwerking in een praktisch te hanteren afsprakenstelsel.

C5. Privacy by design en privacy by default

Doel In deze module worden de principes van privacy by design en default nader toegelicht. Ingegaan wordt op de achtergrond, de bedoeling en de betekenis van deze principes. Deelnemers aan deze module kunnen deze principes zodanig vertalen naar hun eigen organisatie dat de middelen waarmee verwerkingen van persoonsgegevens worden gevoerd alsmede de verwerkingen zelf voldoen aan deze principes. Ook kunnen zij de middelen waarmee verwerkingen van persoonsgegevens worden gevoerd en de bijbehorende procedures en maatregelen beoordelen naar de mate waarin zij voldoen aan de principes van privacy by design en default. Tevens zijn zij in staat de eisen te formuleren in bijvoorbeeld aanbestedingsprocedures voor de aanschaf of ontwikkeling van informatiesystemen.

Duur Een dagdeel

C6. Bewaartermijnen

Doel Na deelname aan dit onderdeel kunnen deelnemers beoordelen of de bewaartermijnen die gelden voor de verschillende verwerkingen van persoonsgegevens voldoen aan de eisen van de Avg. Ook zijn zij in staat om de eisen te formuleren die vanuit privacywetgeving aan het bewaren en vernietigen van gegevens worden gesteld. Dit is tevens van belang in het kader van aanbestedingsprocedures voor de aanschaf of ontwikkeling van informatiesystemen die moeten voldoen aan de hiervoor genoemde principes van privacy by design en default. Tevens kunnen de deelnemers beoordelen of de procedures en maatregelen voldoende zijn om te bewerkstelligen dat persoonsgegevens niet langer bewaard worden dan noodzakelijk voor de doeleinden waarvoor zij worden verzameld en verwerkt en dus tijdig worden vernietigd.

Duur Een dagdeel

C7. Dataportabiliteit

Doel Wanneer persoonsgegevens elektronisch en in een gestructureerd en algemeen gebruikt formaat worden verwerkt, heeft de betrokkene het recht om van de verantwoordelijke een kopie te krijgen. Ook heeft de betrokkene het recht om zijn persoonsgegevens en alle andere informatie die hij heeft verstrekt en door verantwoordelijke worden bewaard, in een algemeen gebruikt elektronisch formaat over te dragen naar een ander geautomatiseerd verwerkingssysteem, zonder daarbij te worden belemmerd. Het is een recht om rekening mee te houden bij de aanschaf en ontwikkeling van informatiesystemen. Het is immers technisch niet altijd op voorhand mogelijk dit recht te effectueren. Deelnemers aan deze module weten met welke eisen zij rekening dienen te houden om het recht van betrokkenen om hun gegevens op te vragen en mee te nemen. Ook kunnen zij de eisen formuleren voor de inrichting van de vastlegging van de persoonsgegevens op een zodanige wijze dat het mogelijk is om aan het recht van

betrokkenen op dataportabiliteit invulling te geven. Voor de eigen organisatie kunnen deelnemers een “beleid voor dataportabiliteit” opstellen.

Duur Een dagdeel

C8. Profiling

Doel Profiling is slechts in bepaalde gevallen toegestaan. Deelnemers die dit onderdeel gevolgd hebben weten wat profiling inhoudt, in welke gevallen onder welke voorwaarden profiling is toegestaan, en welke procedures en maatregelen getroffen moeten worden om aan de regels die de Avg stelt aan profiling te kunnen voldoen. De deelnemer aan de module is in staat het privacybeleid en compliancebeleid zodanig in te richten dat en te beoordelen of aan de voorwaarden op dit punt wordt voldaan. Ook zal de verantwoordelijke zijn informatiebeleid moeten aanpassen aan de Avg alsook het bewijs zodanig moeten vastleggen dat hij kan aantonen aan de Avg te voldoen.

Duur Een dagdeel

D Assessment en audit

Om te beginnen zal in de D module de PSA diepgaand bekeken worden. De methodologie komt aan bod en er wordt inzicht gegeven in de werking van het Standard Business Compliance Managementsysteem (SBCM). SBCM is de feitelijke operationele ondersteuningstool voor PSA. Daarna komt aan de orde hoe het opgezette systeem beoordeeld en getoetst kan worden. Assessments en audits zijn daar het middel voor. In de Avg is de gegevensbeschermingseffectbeoordeling (ofwel PIA) de belangrijkste uitwerking van een assessment. Met een PIA kan voorafgaand aan een verwerking ingeschat worden waar de risico's liggen. Met deze kennis is het mogelijk om de risico's te beperken. Ingegaan wordt op vragen als: in welke situaties moet een PIA worden uitgevoerd; hoe wordt een PIA uitgevoerd; hoe kun je toezicht houden op de uitvoering van een PIA, en hoe kun je de resultaten beoordelen en hiernaar handelen binnen hun organisatie.

D1. Accounting

Doel De Wbp en de Avg vereisen dat de verantwoordelijke bepaalde verwerkingen registreert. Dit is van belang voor de accountant en zijn jaarrekening. Om die reden komen enkele accountants principes en beginselen aan de orde. Tevens komt aan de orde wat, hoe en waarin gedocumenteerd moet worden. Deze module betreft een nadere uitwerking van de Privacy & Security Accounting (PSA) methodologie en er wordt inzicht gegeven in de werking van het Standard Business Compliance Managementsysteem (SBCM). SBCM is de feitelijke operationele ondersteuningstool voor PSA.

Duur Een dagdeel

D2. Assessments

Doel Een PIA (ofwel gegevensbeschermingseffectbeoordeling) wordt in de Avg voor sommige situaties impliciet of expliciet verplicht gesteld. Voor het voeren van cameratoezicht of verwerkingen met gezondheidsgegevens van patiënten bijvoorbeeld wordt het uitvoeren van een PIA verplicht. Voor het bepalen van het profiel van een FG is het voorafgaand uitvoeren van een PIA impliciet verplicht. Voor het ontwikkelen van beleid en wetgeving waar grote hoeveelheden persoonsgegevens mee gemoeid zijn, is het uitvoeren van een PIA sinds 1 september 2013 voor de rijksdienst ook verplicht. Na deze cursus kennen deelnemers de verschillende soorten PIA's, kunnen ze de noodzaak en opzet van een PIA bepalen voor verschillende organisatie specifieke situaties en zijn ze in staat een PIA uit te voeren en de uitkomsten daarvan te beoordelen. Tevens kunnen ze toezicht houden op de uitvoering van de PIA en de resultaten beoordelen en hiernaar handelen binnen hun organisatie.

Duur Een dagdeel

D2a Assessments wettelijk kader, soorten en betekenis

In deze eerste module van cluster D2 wordt de noodzaak en opzet van een Privacy Impact Assessment (PIA) voor verschillende situaties aan de orde gesteld. Ingegaan wordt op vragen als: in welke situaties moet een PIA worden uitgevoerd; hoe wordt een PIA uitgevoerd; hoe kun je toezicht houden op de uitvoering van een PIA, en hoe kun je de resultaten beoordelen en hiernaar handelen binnen hun organisatie?

D2b Assessment, een uitwerking

Deze module bouwt voort op module D2a waarin de noodzaak en uitvoering van een Privacy Impact Assessment (PIA) is toegelicht. In deze module worden trends en ontwikkelingen besproken en gaan we in op structurele inbedding van de PIA in de bedrijfsvoering.

D3. Van Assessments naar Auditing

Doel Deze module betreft een nadere uitwerking van Auditing in de Privacy & Security Accounting (PSA) methodologie. Er wordt inzicht gegeven in de betekenis van het kunnen vaststellen van de effectieve werking van geautomatiseerde processen. Vanuit de Internationale standaards voor Accountants wordt verbinding gelegd met de rol van de Accountant/Auditor.

Duur Een dagdeel

Overzicht, kosten en tijdsbesteding Leergang FG

Cursusonderwerpen			Dagdelen
A	**Formeel Juridisch**		
A1		**De inleiding omtrent privacy**	**3**
	A1a	Overzicht van de huidige privacywetgeving	
	A1b	De Avg, de nieuwe privacyregels	
	A1c	Overzicht in wetgeving rond beveiliging en identitymanagement	
A2		**De e-privacyverordening**	**1**
A3		**De Avg in internationaal perspectief**	**2**
	A3a	De Avg in een internationaal perspectief: Europa	
	A3b	De Avg in een internationaal perspectief: V.S., verre oosten en rest van de wereld	
A4		**Privacy en aanpalende wetgeving**	**1**
B	**Governance & Compliance**		
B1		**De FG, taken bevoegdheden en verantwoordelijkheden**	**1**
B2		**De Avg, en privacy beleid, policy privacy framework en -baseline**	**2**
	B2a	Privacybeleid: Policyframework, normenkader en privacyorganisatie	
	B2b	Intern en extern privacybeleid	
B3		**Governance & Compliance**	**2**

	B3a	Governance & Compliance – wetgeving in breder perspectief	
	B3b	Governance & Compliance – nader uitgewerkt	
B4		**Datalekken en nu?**	**2**
	B4a	Voorbereid zijn op een datalek	
	B4b	Hoe kan en moet ik handelen na een datalek?	
C	**Materieel, opzet, bestaan en werking van maatregelen en mechanismen**		
C1		**Overzicht & inzicht in de verantwoordelijkheden & aansprakelijkheden**	1
C2		**Transparantie en effectueren van rechten aan betrokkenen**	1
C3		**Informatiebeveiliging de basis voor privacybescherming**	2
	C3a	Informatiebeveiliging, de basis voor privacybescherming	
	C3b	Informatiebeveiliging, verdieping	
C4		**Lifecycle privacy protection management**	4
	C4a	Lifecycle privacy protection management	
	C4b	Architecturen en uitgangspunten	
	C4c	Modellen voor Attribute Based Credentials	
	C4d	Inregelen van afsprakencomplex	
C5		**Privacy by design & privacy by default**	1
C6		**Bewaartermijnen**	1
C7		**Dataportabiliteit**	1
C8		**Profiling**	1
D	**Assessment en audit**		

D1		**Accounting**	1
D2		**Assessments**	2
	D2a	Assessments wettelijk kader, soorten en betekenis	
	D2b	Assessment, een uitwerking	
D3		**Assessment → Auditing**	1
Totaal aantal modulen			**30**
	Zelfstudie		480
	Deelname workshops		120
Totale studiebelasting			**600**

Deze persoonlijke leerweg omvat 30 dagdelen à € 500: € 15.000 exclusief reiskosten en BTW. De studiebelasting van dit studieprogramma bedraagt 600 uur en bestaat uit: deelname cursus op locatie Frankenslag en zelfstudie.