Verslag bijeenkomst KNR – AVG
26 september 2018

1. Opening
De heer Crajé heet de aanwezigen welkom. In deze bijeenkomst zal de heer Rik Geurts, advocaat bij Van Iersel Luchtman Advocaten, ingaan op een aantal zaken rond de Algemene Verordening Gegevensbescherming (AVG). Op 28 juni 2018 heeft al een bijeenkomst over de AVG plaatsgevonden. De belangstelling voor dit onderwerp was zo groot dat besloten is de heer Geurts te vragen nogmaals op dit onderwerp in te gaan. Op deze bijeenkomst wordt een basiskennis van de AVG verondersteld en zal de heer Geurts vooral ingaan op vragen van de aanwezigen.

De heer Crajé geeft het woord aan de heer Geurts.

2. Presentatie AVG

De heer Geurts dankt de heer Crajé voor de gelegenheid om wederom het een en ander toe te lichten over de AVG. Hij zal graag ingaan op vragen van de aanwezigen. De vorige keer waren er voornamelijk hogere oversten aanwezig; nu zijn het beleids- en stafmedewerkers. De heer Geurts verwacht daarom een ander soort vragen dan op 26 juni 2018. Voor zijn presentatie gebruikt hij dezelfde PowerPoint presentatie als op 26 juni 2018 (de volledige presentatie vindt u hier).

De heer Geurts is partner bij Van Iersel Luchtman Advocaten. Hij is sectiehoofd van de sectie Intellectueel Eigendom (IE), IT & Privacy en houdt zich uit dien hoofde bezig met de AVG. De heer Geurts houdt zich hoofdzakelijk bezig met het privacyrecht. Privacy is een onderwerp waar veel over te doen is tegenwoordig. De afdeling bij Van Iersel Luchtman Advocaten is in één jaar tijd gegroeid van twee naar vijf medewerkers.

Sheets 1 – 3
- Vandaag zal gesproken worden over een aantal aspecten van de AVG. De interactieve discussie staat voorop; het is niet de bedoeling dat de heer Geurts een lezing over de AVG geeft. Na 26 juni 2018 heeft hij een heel aantal aanvullende vragen ontvangen. Hij zal trachten deze gedurende de bijeenkomst te beantwoorden. Onderwerpen die de revue zullen passeren zijn:
  - ✓ Wat is privacy? Waar gaat het precies om? Wat valt onder het begrip privacy?
  - ✓ Privacy regelgeving en enkele kernbegrippen.
  - ✓ Belangrijk(st)e wijzigingen in de AVG.
  - ✓ De AVG en religieuze gemeenschappen en verenigingen. Wat is er veranderd voor deze specifieke doelgroep?
  - ✓ Aanpak en vragen. Er is een stappenplan uitgewerkt door de Autoriteit Persoonsgegevens (APG).

Sheets 4 – 8
- Privacy is het beschermen van de eigen levenssfeer; ervoor zorgen dat anderen deze levenssfeer eerbiedigen. Een definitie van privacy is ‘het recht met rust gelaten te worden; het recht op een persoonlijke levenssfeer’. Het recht op privacy is vastgelegd in de Grondwet. Privacy is belangrijk omdat:
  - ✓ Onze maatschappij steeds meer en sneller gedigitaliseerd raakt. Data groeit exponentieel en kan op steeds meer wijzen gebruikt worden.
  - ✓ Het gebruik en delen van persoonsgegevens is niet meer weg te denken uit ons zakelijk en privé bestaan.
  - ✓ De impact van het gebruik van data op personen wordt steeds groter.
- Omdat er steeds grotere schaal data verzameld wordt, zijn er regels nodig om dit te reguleren. Dit is de kern van de privacyregelgeving. Deze wetgeving is onder andere bedoeld om ons als persoon een controlemechanisme te geven over wat met onze persoonsgegevens gebeurt. De

AVG zorgt voor bedrijven en organisaties veel werk, maar levert aan de andere kant ook controlemogelijkheden op.

Sheets 9 – 11

- De Algemene Verordening Gegevensbescherming (AVG) vervangt de Wet bescherming persoonsgegevens (Wbp).
- De AVG is van toepassing vanaf 25 mei 2018.
- De Wpb is vervallen per 25 mei 2018. De Uitvoeringswet AVG, aangenomen op 16 mei 2018, regelt samengevat de intrekking van de Wpb, de grondslag voor het bestaan van de Autoriteit Persoonsgegevens en de grondslag voor het invullen van de open normen in de AVG.
- De AVG is eigenlijk breder / uitgebreider dan de Wpb; het biedt een uitgebreider pallet aan sancties.

Sheet 12; deel 1

- Een persoonsgegeven is elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Steeds meer gegevens worden gezien als persoonsgegevens. Bij alles moet je de vraag stellen 'is dit een persoonsgegeven of kan het een persoonsgegeven worden?'. Dit laatste kan het geval zijn door koppeling met andere gegevens. Een gegeven dat op zichzelf niet herleidbaar is tot een persoon kan in combinatie met een ander gegeven ineens wel een persoonsgegeven worden.
- De betrokkene is de persoon om wie het gaat. Degene wiens gegevens het betreft. De verwerkingsverantwoordelijke is de organisatie die de gegevens verzamelt en het doel en de middelen van de verwerking bepaalt. De verwerker handelt in opdracht van de verwerkingsverantwoordelijke. De verwerker bepaalt niet zelf het doel van zijn handelen; de verwerker mag niet buiten zijn opdracht treden. Wanneer dit wel gebeurt wordt de verwerker eigenlijk aangemerkt als verwerkingsverantwoordelijke en moet hij uit dien hoofde de AVG nalezen. Hier loopt het vaker spaak.

Deze informatie levert een aantal vragen op:

- *Wanneer een zorgmedewerker wondmateriaal besteld voor mevrouw X, is deze zorgmedewerker dan verwerker of verwerkingsverantwoordelijke?*

  Bij de AVG gaat het om persoonsgegevens. Gegevens die herleidbaar zijn tot een persoon. Worden er bij de bestelling geen persoonsgegevens verwerkt door de zorgmedewerker (het gaat bijvoorbeeld om een grote algemene bestelling), dan is de AVG niet hierop van toepassing. Worden er bij de bestelling wel persoonsgegevens verwerkt, dan is de AVG wel van toepassing. In dit geval moet je gaan kijken hoe de zorgmedewerker handelt. Handelt de zorgmedewerker zelfstandig bij de bestelling (dus niet in opdracht van mevrouw X) en bepaalt de zorgmedewerker zelf welke persoonsgegevens worden verwerkt, dan is de zorgmedewerker verwerkingsverantwoordelijke.

  Voorts is het van belang dat binnen de organisatie van de verwerkingsverantwoordelijke (lees: de zorgmedewerker) deze verwerkingsverantwoordelijkheid wordt vastgelegd.

  Tot slot speelt dat een apotheek verplicht is te verifiëren of jij gemachtigd bent om deze zaken te bestellen en op te halen voor mevrouw X. Zij mogen het namens mevrouw X bestelde niet zomaar aan de zorgmedewerker meegeven.

- *Het is nog niet helemaal duidelijk waarom deze zorgmedewerker als verwerkingsverantwoordelijke en niet als verwerker wordt aangemerkt. Ze handelt toch in opdracht van mevrouw X?*

  Als de zorgmedewerker het doel en middelen van hetgeen besteld wordt, bepaalt, dan is de zorgmedewerker verwerkingsverantwoordelijke.

- *Vaak is een bestelprocedure digitaal. Via de arts levert een apotheek de bestelde middelen af. Hoe zit het dan met de benodigde toestemming? En mogen de bestellingen bij de receptie afgegeven worden of moeten zij door de besteller in ontvangst genomen worden?*

Ook bij een gedigitaliseerde bestelprocedure zal vastgelegd moeten worden wie gemachtigd is bestellingen te doen. De relatie tussen besteller, zorgvrager, arts en apotheek dient beschreven te worden. Bestellingen kunnen alleen bij de receptie afgegeven worden wanneer de medewerkers een verklaring van geheimhouding hebben ondertekend.

- *Hoe zit het in het geval dat een medewerker een bestelling doet namens zijn werkgever?*
  Wanneer een medewerker in opdracht van zijn werkgever handelt is de werkgever verwerkingsverantwoordelijke. In de arbeidsovereenkomst dient dan wel te zijn vastgelegd dat de medewerker namens de werkgever mag optreden. Overigens blijft de medewerker wel aanspreekbaar op zijn acties.

- *De heer Geurts wijst erop dat, wanneer er gewerkt wordt met ZZP-ers, het privacybeleid apart vastgelegd dient te worden. ZZP-ers werken met een Overeenkomst van Opdracht. Formats hiervan, voorzien van een verwijzing naar het privacybeleid, staan op de website van de R.K.-kerk.*

<u>Sheet 12; deel 2</u>

- De grondslagen voor verwerking zijn:
  - ✓ Toestemming.
  - ✓ Noodzakelijk voor de uitvoering van de overeenkomst.
  - ✓ Noodzakelijk voor de uitvoering van een gerechtvaardigd belang. Dit is onder andere het geval bij het overnemen van een klantenbestand. Dan heb je bepaalde gegevens nodig.
  - ✓ Noodzakelijk voor de uitvoering van een wettelijke verplichting. Administratieve gegevens dienen zeven jaar bewaard te worden. Alle gegevens die je niet nodig hebt om aan je wettelijke verplichting te voldoen zullen vernietigd moeten worden. Gegevens van een medewerker mag je gedurende de arbeidsovereenkomst bewaren. Na uitdiensttreding dient het personeelsdossier na twee jaar vernietigd te worden, met uitzondering van de gegevens die je nodig hebt om aan je wettelijke verplichting te voldoen.
  - ✓ Noodzakelijk voor de uitvoering van een vitaal belang.
  - ✓ Noodzakelijk voor de uitvoering van een algemeen belang.
- Artikel 9 van de AVG gaat in op de archivering. In lid 2 sub j is het volgende bepaald: *'De verwerking is noodzakelijk met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden overeenkomstig artikel 89, lid 1, op grond van Unierecht of lidstatelijk recht, waarbij de evenredigheid met het nagestreefde doel wordt gewaarborgd, de wezenlijke inhoud van het recht op bescherming van persoonsgegevens wordt geëerbiedigd en passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de belangen van de betrokkene.'.* Bij archivering dien je altijd het nagestreefde doel in het oog te houden. Een personeelsdossier mag je niet archiveren tenzij archivering een statistisch doel beoogd. Dit statistische doel kan echter bereikt worden door een opgeschoond dossier te archiveren. Per archiefcategorie zal gekeken moeten worden welke gegevens noodzakelijk zijn om te bewaren en welke vernietigd moeten worden. Dit geldt niet alleen voor de papieren, maar zeker ook voor de digitale gegevens.

Dit onderwerp levert een aantal vragen op:

- *Mag je gegevens wel bewaren wanneer je hiervoor toestemming vraagt aan degene die het betreft?*
  Met het vragen van toestemming kun je inderdaad wel het een en ander ondervangen. Maar zeker niet alles. Er zal altijd naar het doel gekeken moeten worden. Gegevens van een sollicitant mag je tot 2 weken na de sollicitatie bewaren. In overleg kan je de gegevens echter tot maximaal één jaar in portefeuille houden. Maar wanneer je samen overeenkomt dat de gegevens 30 jaar bewaard mogen worden is er weliswaar sprake van toestemming, maar toch zal dit niet rechtsgeldig zijn. Het 30 jaar bewaren van deze gegevens dient geen enkel doel en zal niet rechtsgeldig zijn.

- *Bij de Missiezusters van OLV van Afrika is aan alle zusters toestemming gevraagd om persoonsgegevens te mogen bewaren. Deze gegevens zijn van belang voor het nageslacht; voor tentoonstellingen over hun missiewerk. Deze gegevens zijn persoonsgegevens omdat ze te herleiden zijn naar individuele zusters.*

  De heer Geurts antwoordt dat er altijd gekeken moet worden naar de soort gegevens en het doel. Wanneer het gaat om gegevens, foto's, van zusters in een missiegebied kan het bewaren van deze gegevens een historisch doel dienen. Dit soort doelstellingen zal je in je privacybeleid moeten vastleggen. Concretiseer welke gegevens van welke groep personen met welk doel je wilt bewaren. En bepaal per doel welke bewaartermijn passend is. De religieuzen van wie je gegevens wilt bewaren met het oog op een historisch doel, dienen hiervan op de hoogte gesteld te worden. Ze moeten toestemming geven en ook een controlemogelijkheid geboden worden. Ze moeten kunnen controleren of de bewaartermijnen en het doel nageleefd worden en moeten kunnen ingrijpen wanneer afgeweken wordt van het vooraf bepaalde doel of wanneer de overeengekomen termijn overschreden wordt.

- *De Augustinessen van Sint Monica hebben altijd kwetsbare meisjes opgevangen in Meisjesstad. Deze maatschappelijke opvang werd in 1939 gesticht door de zusters en was aanvankelijk alleen bedoeld als opvang voor jonge meisjes die ongewenst zwanger waren geworden. Soms kloppen mensen aan bij de zusters omdat ze op zoek zijn naar hun roots. Ze zoeken gegevens over hun moeder die in Meisjesstad is opgevangen. De gegevens van de moeders zijn opgetekend in een inschrijfboek. De gegevens hierin mogen dus niet met de kinderen gedeeld worden? Ze kunnen dan niet meer geholpen worden.*

  De heer Geurts antwoordt dat er bij dergelijke vragen onderscheid gemaakt moet worden in de persoon die het vraagt. Wanneer een persoon betrokken is, een kind van één van de meisjes, heeft rechten en mag die rechten ook uitoefenen. Dit kan door informatie op te vragen bij de zusters. De heer Willemsen (Zusters van Liefde Tilburg) vult dit aan. In de jaren '90 van de vorige eeuw is een rechtszaak gevoerd over het recht van kinderen om te weten wie hun biologische ouders zijn. De rechter heeft bepaald dat kinderen inzage mogen krijgen in de gegevens wanneer die bewaard zijn gebleven. Het is hun recht om te weten van wie ze afstammen. De heer Geurts beaamt dit, maar de gegevens moeten dan wel bewaard zijn gebleven. Wanneer dit het geval is zal je per vraag moeten kijken of je inzage mag geven. Bij een direct betrokkene is het duidelijk; een kind heeft recht op inzage. Wordt de vraag echter gesteld door een niet direct betrokkene, een familielid bijvoorbeeld, dan gaat het belang van degene van wie de persoonsgegevens zijn voor. Er zal dus altijd doorgevraagd moeten worden en per vraag bepaald moeten worden of inzage gegeven kan worden. Hierbij kan een belangenafweging plaatsvinden.

<u>Sheet 12; deel 3</u>

- Doel en doelbinding. Doelen van verwerking van persoonsgegevens dienen goed omschreven te worden. Deze omschrijving dient concreet te zijn; voldoende ruim maar niet te ruim. Wanneer je later besluit een doel uit te breiden kan dit alleen wanneer de uitbreiding verbonden is met het oorspronkelijke hoofddoel.
- Verwerking van persoonsgegevens die niet voldoen aan het omschreven doel is niet toegestaan.
- Een organisatie dient de technische systemen te beveiligen. De mate van beveiliging mag in overeenstemming zijn met de mogelijkheden die een organisatie heeft. Een investering in de beveiliging hoeft niet buitenproportioneel te zijn. Er zal echter wel altijd sprake moeten zijn van een tweewegverificatie. Bijvoorbeeld, wanneer je een wachtwoord wilt wijzigen zal je moeten zorgen dat dit verzoek gecontroleerd wordt door middel van een SMS met inlogcode.

<u>Sheets 13 + 14</u>

- Een IP-adres is een persoonsgegevens omdat het gekoppeld is aan een computer. Deze kan herleid worden tot een persoon. De Autoriteit Persoonsgegevens heeft bepaald dat een IP-adres een persoonsgegeven is.

- Een gezicht is ook een persoonsgegeven. Ook wanneer een gezicht in eerste instantie niet herkenbaar lijkt te zijn. Zoals het hoofd op de rechterfoto. Dat is van de achterkant gefotografeerd en lijkt niet herkenbaar. Met de huidige mogelijkheden van fotoherkenningssoftware is het mogelijk om te achterhalen om wie het gaat. Bijvoorbeeld doordat op Facebook ook de voorkant van dit hoofd staat en er een link gelegd kan worden door het herkenningssysteem.

<u>Sheets 15 – 18</u>

- De belangrijkste wijzingen AVG zijn:
  - ✓ Het centrale begrip persoonsgegevens is ruimer. Steeds meer gegevens worden als persoonsgegeven aangemerkt omdat ze in combinatie met elkaar herleidbaar zijn naar een persoon.
  - ✓ Het privacybeleid moet nog uitgebreider. Alles moet vastgelegd worden, maar wel kort en bondig. Sommige webshops hanteren een enorm lange privacyverklaring en nemen hier hele wetteksten in op. Dit doen ze om zichzelf in te dekken, maar tegelijkertijd weten ze dat niemand meer dan 1 A-4 gaat lezen.
  - ✓ Versterking van de rechten van betrokkenen. Een voorbeeld hiervan is het digitale patiëntendossier. Wanneer je gaat verhuizen kan je dit opvragen en aan je nieuwe huisarts verstrekken.
  - ✓ Versterking van verantwoordelijkheden van organisaties die persoonsgegevens verzamelen en gebruiken. Hiertoe behoort het recht om vergeten te worden. Wanneer je bij een werkgever vertrekt kan je eisen dat alles wat naar jou verwijst verwijderd wordt. Bijvoorbeeld foto's van een bedrijfsuitje waar je op staat of een foto van jou op een brochure. Digitaal vergeten worden is lastiger. Online zijn altijd gegevens over iemand te vinden. Wanneer je wilt dat een zoekmachine bepaalde gegevens van jou niet meer zichtbaar maakt, kan je bij Google een verzoek tot verwijdering indienen. Google zal dan een belangenafweging maken; het belang van het individu versus de vrijheid van meningsuiting. In het uiterste geval kan de rechter gevraagd worden hierover een uitspraak te doen. Ook de verplichting tot het melden van datalekken valt hieronder.
  - ✓ Het aanstellen van een Functionaris Gegevensbescherming (FG). Deze functionaris is verplicht wanneer op grote schaal gevoelige persoonsgegevens worden verwerkt. Een organisatie zal een inschatting moeten maken of een FG in hun geval verplicht is. De FG is het aanpreekpunt voor de AVG. Gekozen kan worden voor een externe FG maar ook voor een medewerker. In dat laatste geval zal wel gewaarborgd moeten worden dat de FG kan functioneren zonder dat zijn of haar handelen in het kader van de AVG consequenties heeft. Een FG wordt wettelijk beschermd en mag niet ontslagen worden vanwege zijn of haar handelen met betrekking tot de AVG. Een FG moet neutraal kunnen kijken naar eventuele pijnpunten en deze kunnen benoemen zonder dat het consequenties heeft. Een FG heeft de plicht over deze pijnpunten te rapporteren aan de Autoriteit Persoonsgegevens. Het is echter beter om deze pijnpunten eerst intern bespreekbaar te maken en met de organisatie naar oplossingen te zoeken.
  - ✓ Het contoleren en vastleggen van afspraken met verwerkers.
  - ✓ Accountability. Organisaties zijn verplicht een verwerkingsregister bij te houden. Toestemming voor het bewaren van gegevens dient schriftelijk vastgelegd te worden zodat je kunt bewijzen dat die toestemming ook daadwerkelijk gegeven is. Wanneer je nieuwsbrieven verstuurt moet je de ontvanger toestemming vragen. De ontvanger dient expliciet aan te geven dat de nieuwsbrief toegestuurd mag worden.
  - ✓ Data Protection Impact Assessment (DPIA). Dit is een instrument om vooraf de privacyrisico's van gegevensverwerking in kaart te brengen en vervolgens maatregelen te kunnen nemen om risico's te verkleinen. Het DIPA is een risicotest Artikel 35, lid 3 heeft hier betrekking op en luidt als volgt:

    3. Een gegevensbeschermingseffectbeoordeling als bedoeld in lid 1 is met name vereist in de volgende gevallen:

    a) een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon

rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen;

b) grootschalige verwerking van bijzondere categorieën van persoonsgegevens als bedoeld in artikel 9, lid 1, of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10; of

c) stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.

Lid a) en b) zijn hoogstwaarschijnlijk niet van toepassing op religieuze instituten. Wel zal in het kader van lid b) nagedacht moeten worden over de inhoud van het begrip 'grootschalige verwerking'. Is er sprake van grootschalige verwerking bij een paar honderd of een paar duizend? Wanneer je inschat dat je te maken hebt met grootschalige verwerking is het beter toch een FG aan te stellen. Lid c) zou van toepassing kunnen zijn. Er kan sprake zijn van openbaar toegankelijke ruimten die geobserveerd en gemonitord worden. Bijvoorbeeld een openbare parkeerplaats met cameratoezicht. Dat er sprake is van camerabewaking zal je duidelijk aan moeten geven.

- ✓ Versteviging van de onafhankelijkheid en bevoegdheden van de nationale autoriteiten. Ook kan de Autoriteit Persoonsgegevens hoge boetes opleggen bij overtreding van de AVG. Het kan dan gaan om boetes tot 20 miljoen euro of 2% van je wereldwijde omzet. Wanneer je een holding bent met een aantal dochters en één van de dochters krijgt een boete, dan wordt alle omzet meegerekend. Dit kan tot enorme boetes leiden. Overigens is het traject naar een daadwerkelijke boete lang. Eerst zal er, naar aanleiding van een melding, onderzoek gedaan worden, daarna zal gesproken worden met de organisatie die in de fout gaat en zal gevraagd worden het privacybeleid aan te passen. Indien dit niet gebeurt zal een aanzegging tot boete gedaan worden en wanneer de organisatie dan nog hun beleid niet verbetert zal er een boete opgelegd worden door de Autoriteit Persoonsgegevens. Sinds 1 januari 2016 is nog geen enkele boete opgelegd.

De volgende vragen worden gesteld:

- *Wat moet je precies verstaan onder het begrip 'op grote schaal gevoelige persoonsgegevens verwerken'?*

  De AP heeft de richtlijn voor grootschaligheid in de zorg nader ingevuld. Voor huisartsenpraktijken en instellingen voor medisch specialistische zorg, niet zijnde ziekenhuizen, geldt dat een verwerking grootschalig is als:
  - die praktijk of instelling meer dan 10.000 patiënten heeft ingeschreven óf als die gemiddeld meer dan 10.000 patiënten per jaar behandelt
  - én de gegevens van deze patiënten in één informatiesysteem staan.

  De verwerking van patiëntgegevens door ziekenhuizen, zorggroepen, huisartsenposten en apotheken (behalve als er sprake is van een solistisch werkende zorgverlener) is altijd grootschalig.

  Er zijn uiteraard nog veel andere zorgaanbieders. Voor deze zorgaanbieders geldt het criterium van 10.000 patiënten niet. Deze organisaties moeten aan de hand van vier factoren zelf beoordelen of zij grootschalig gegevens verwerken.

- *Dienen religieuze instituten een FG aan te stellen?*

  Dit zal ieder religieus instituut zelf moeten overwegen. Religie is een persoonsgegeven, maar het maar de vraag of dit gegeven op grote schaal wordt verwerkt. Wellicht is het toch verstandig om een persoon binnen de organisatie aan te wijzen als FG ook al is dit formeel misschien niet verplicht. Deze persoon kan dan fungeren als aanspreekpunt AVG en privacyvragen. Opgemerkt wordt dat het voor de hand ligt om de gegevensverantwoordelijke FG te maken.

- *Reageert de Autoriteit Persoonsgegevens alleen op klachten of worden er ook steekproeven genomen?*

  De Autoriteit Persoonsgegevens is een handhavingsautoriteit. Dat betekent dat ze zowel zelf onderzoek kunnen doen als op klachten kunnen reageren. Ze kunnen naar de markt kijken en steekproeven uitvoeren in een bepaalde sector. Op dit moment contro-

leren ze overheid, zorg en de financiële sector. Al deze sectoren dienen een FG aangesteld te hebben. Of dit daadwerkelijk gedaan is, is makkelijk te controleren aangezien een FG aangemeld moet worden bij de Autoriteit Persoonsgegevens. De Autoriteit Persoonsgegevens treedt autonoom op. Ze bepalen zelf of ze onderzoek doen. Ze geven helaas geen advies. Het is dus afwachten wat er uit de controles komt. Wellicht kan hieruit lering getrokken worden. Ook de dataverwerking van Facebook is wordt door hen onderzocht. In Spanje is dit ook gedaan en daar is wel een boete uitgedeeld.

Sheets 19 – 21

- De AVG bouwt voort op de Wpb; de uitgangspunten zijn hetzelfde. Bestaande regelingen dien je in overeenstemming met de normen van de AVG te brengen.
- In de AVG wordt rekening gehouden met de bijzondere positie van kerken en kerkgenootschappen. Dit betekent niet dat aan deze genootschappen geen verplichtingen in het kader van de AVG worden opgelegd, maar dat er rekening gehouden wordt met het in de Grondwet vastgelegde recht op vrijheid van godsdienst en levensovertuiging.

Sheets 22 – 24

- Er is veel informatie, onder andere het 10-stappenplan) te vinden op de website van de Autoriteit Persoonsgegevens; www.autoriteitpersoonsgegevens.nl
- Deze stappen zijn:
  - ✓ Stap 1 = Bewustwording. Hoe maak ik iedereen in mijn organisatie bekend met de regels van de AVG. Zorg dat je gegevens beveiligd zijn en dat de kasten op slot zijn.
  - ✓ Stap 2 = Rechten van betrokkenen. Informeer iedereen over zijn of haar rechten in het kader van de AVG en waarborg dat iedereen de eigen privacyrechten kan uitoefenen.
  - ✓ Stap 3 = Overzicht van verwerkingen. Breng de gegevensverwerking in kaart. Wat verwerkt u en met welk doel? De essentie van de AVG is controle; je kunt pas controle uitoefenen wanneer je deze vragen kunt beantwoorden.
  - ✓ Stap 4 = DPIA. Controleer of je een DPIA moet uitvoeren. Voer de testen voor een DPIA en een FG uit en neem een besluit op basis van de resultaten. En leg dat besluit ook schriftelijk vast.
  - ✓ Stap 5 = Privacy by Design & Default. Default is dat je alles op nul zet. Je verwerkt geen gegevens tenzij. Vanaf nul ga je nadenken over welke gegevens je moet gaan verwerken en met welk doel.
  - ✓ Stap 6 = FG. Dit onderwerp is zojuist al uitgebreid besproken.
  - ✓ Stap 7 = Meldplicht datalekken. De verplichting om datalekken te melden is niet gewijzigd en blijft van kracht. Wel worden er hogere eisen gesteld aan de eigen registratie van de datalekken die zich in de organisatie hebben voorgedaan. Een organisatie dient de beveiligingsincidenten te registreren en vervolgens een beslissing te nemen over het al dan niet melden bij de Autoriteit Persoonsgegevens. De organisatie neemt zelf deze beslissing, maar dient de beslissing wel te kunnen motiveren. Wanneer een datalek niet gemeld wordt terwijl dat gedaan had moeten worden kan een boete opgelegd worden. In de praktijk zal echter eerst een waarschuwing gegeven worden.
  - ✓ Stap 8 = Verwerkingsovereenkomsten. Hierin wordt vastgelegd hoe je als organisatie omgaat met persoonsgegevens. Het gaat om een overeenkomst tussen verwerkingsverantwoordelijke en verwerker. Wanneer je persoonsgegevens in de Cloud bewaart heb je een verwerkingsovereenkomst met Microsoft. Microsoft mag niets doen met jouw gegevens tenzij je hiervoor toestemming geeft. Wanneer jouw gegevens in de Cloud misbruikt worden, kan je Microsoft aansprakelijk stellen.

De volgende vragen worden gesteld:

- *Wie stelt de verwerkingsovereenkomst op?*

  Onder de Wpb was dit de verwerkingsverantwoordelijke. In de AVG wordt hierover geen duidelijke uitspraak gedaan, maar de AVG kent wel de verplichting dat verwerkingsverantwoordelijke en verwerker een verwerkersovereenkomst moeten hebben. Hebben zij deze niet, dan zijn zij beiden in overtreding van de AVG en kan de AP aan beide eventueel een strafmaatregel opleggen.

- *Moet je met iedereen een verwerkingsovereenkomst opstellen?*

  Nee. Dit is alleen nodig wanneer er sprake is van een verwerkingsverantwoordelijke en een verwerker. Zoals gezegd ben je verwerker als je alleen in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerkt en zelf niet het doel en de middelen van verwerking bepaalt.

  De heer Geurts geeft een tweetal voorbeelden waarbij sprake is van gezamenlijke verwerkingsverantwoordelijkheid (een situatie waarbij geen verwerkersovereenkomst nodig is, maar wel een overeenkomst inzake gezamenlijke verwerkingsverantwoordelijkheid). Wanneer sprake is van een internationale groep ondernemingen die onder één moedermaatschappij in het buitenland vallen. De moedermaatschappij mag de gegevens van de dochter in Nederland opvragen wanneer er sprake is van een gerechtvaardigd belang. Dit kan zijn het bepalen van de salarissen en de vakantiedagen. Nederland dient op verzoek deze gegevens te verstrekken en beide partijen worden aangemerkt als verwerkingsverantwoordelijke. De verstrekker van de gegevens moet verifiëren of de vrager gerechtigd is deze gegevens op te vragen en registreren welke gegevens verstrekt worden. Een ander voorbeeld is een aantal zorgplatformen die samenwerken met overheid en gemeentes. Er worden op de fora vragen gesteld en hulp geboden. Vraag en aanbod worden met elkaar in contact gebracht. De fora wisselen gegevens uit met de overheid en beide partijen, fora en overheid, worden aangemerkt als verwerkingsverantwoordelijke. Er hoeft dus geen verwerkingsovereenkomst opgesteld te worden.

Sheet 25

- Stap 9 = Leidende toezichthouder. Er is sprake van een leidende toezichthouder wanneer een organisatie vestigingen in meerdere EU-lidstaten heeft of de gegevensverwerking in meerdere lidstaten impact heeft. In dat geval is onder de AVG sprake van één privacytoezichthouder; de leidende toezichthouder.
- Stap 10 = Toestemming. Voor sommige gegevensverwerkingen is toestemming van betrokkene vereist. De AVG eist dat u in dit geval een geldige, schriftelijke, toestemming kunt overleggen. Het eventueel intrekken van de toestemming mag niet moeilijk gemaakt worden.

Sheets 26 + 27

De heer Geurts heeft een 13-tal vragen geformuleerd. Een aantal wordt besproken.

- *Wie is de verantwoordelijke voor het melden van een datalek?*

  Dit is de Functionaris Gegevensverwerking van de verwerkingsverantwoordelijke. Wanneer er geen FG vereist is en dus niet is aangewezen, dan is de verwerkingsverantwoordelijke de aangewezen persoon.

- *Hoe moet je handelen wanneer je ziet dat iemand aan je (computer)bestanden heeft gezeten?*

  Wanneer je dit constateert, dien je dit bij je leidinggevende te melden. Ieder beveiligingsincident dient geregistreerd te worden. Vervolgens neemt de FG of de gegevensverantwoordelijke de beslissing dit incident al dan niet te melden bij de Autoriteit Persoonsgegevens.

- *Moeten we alle donateurs van alle projecten die bij ons geadministreerd worden inlichten over hetgeen bij ons geregistreerd staat? Idem voor personeelsleden, oud-personeelsleden en vrijwilligers*

  Alle belanghebbenden dienen ingelicht te worden. Dit kan door middel van een privacyverklaring. Dit is een eenzijdige verklaring die niet ondertekend hoeft te worden. Wel dient de privacyverklaring aan de belanghebbenden bekend gemaakt te worden. Deze verklaring dient minimaal op de website gezet te worden, maar (per mail) toesturen is beter. Dit geldt voor donateurs, (oud)personeelsleden en vrijwilligers, maar ook wanneer je gegevens verzamelt over de bezoekers van je website. Alle belanghebbenden dienen op de hoogte gesteld worden van de privacyverklaring of deze makkelijk te kunnen vinden. Bij

nieuwe medewerkers kan je ervoor kiezen de privacyverklaring toe te voegen aan de arbeidsovereenkomst. Voor welke methode van bekendmaking je ook kiest, zorg ervoor dat je duidelijk bent en dat je kunt bewijzen dat de privacyverklaring onder de aandacht is gebracht.

- *Is voor de website een SSL-certificaat verplicht?*
  SSL is een techniek die overgeseinde data versleutelt. Door de verbeterde technieken volstaat SSL eigenlijk niet meer. Aanbevolen wordt TLS te gebruiken. Het is aan te bevelen hierover met de eigen IT-specialist of met je websitebeheerder te overleggen. Wellicht worden er helemaal geen data overgeseind en is deze zwaardere beveiliging niet noodzakelijk. De AVG eist dat, wanneer er online data-overdracht plaatsvindt, dit ook veilig gebeurt.

- *Moeten we een verwerkingsregister hebben?*
  Ja dit is in principe verplicht voor de meeste organisaties. Per categorie dienen alle verwerkingen genoteerd te worden. Er is een aantal formats van een verwerkingsregisters. Deze zijn bij de heer Geurts op te vragen.

- *Mag je foto's van herkenbare personen op de website, Facebook of in bladen plaatsen? Moet je hiervoor toestemming vragen?*
  Je moet een grondslag voor verwerking hebben. Heb je niets geregeld voor deze verwerking (bijv. bij een privacyverklaring), dan dien je toestemming te vragen..

- *Vallen buitenlandse zusters onder de AVG?*
  Wanneer de persoonsgegevens van deze zusters in Nederland worden bijgehouden en verwerkt valt dit onder de AVG. Wel is het goed om een verwerkingsovereenkomst op te stellen. Welke soort overeenkomst hiervoor nodig is, is afhankelijk van de wijze waarop het gegevensverkeer plaatsvindt. Het kan hier gaan om internationale gegevensuitwisseling. Wanneer het land waarmee je uitwisselt geen passend regime heeft voor de beveiliging van persoonsgegevens en er is met dit land geen verdrag of protocol, dan dient de verwerkingsovereenkomst opgesteld conform het format van de Europese Commissie. Een format van een dergelijke verwerkingsovereenkomst staat op hun website.

<u>Sheets 28 + 29</u>
De heer Geurts geeft aan dat hij graag bereid is vragen met betrekking tot de AVG en privacy te beantwoorden. Hij mag via de KNR of rechtstreeks benaderd worden. Aan de beantwoording van een eenvoudige vraag zijn geen kosten verbonden. Dit ligt natuurlijk anders wanneer er sprake is van een tijdrovende adviesvraag.

3. Sluiting
De heer Crajé dankt de heer Geurts voor zijn bereidheid om zijn kennis over dit onderwerp opnieuw met de achterban van de KNR te delen. Van deze bijeenkomst zal een verslag gemaakt worden. Dit verslag zal op de website van de KNR geplaatst worden. De dank wordt onderstreept met applaus en bloemen.

2019-01-31
Nita van Bergen