Eerste hulp bij privacy!

‘Een praktijkgericht juridisch onderzoek naar de huidige werkwijze met in achtneming van de nieuwe privacywet- en regelgeving’

Amy van de Klundert
Juridische Hogeschool Avans-Fontys te Tilburg
RADAR antidiscriminatiebureau

Tilburg, 9 januari 2018

Eerste hulp bij privacy!

‘Een praktijkgericht juridisch onderzoek naar de huidige werkwijze met in achtneming van de nieuwe privacywet- en regelgeving’

In opdracht van RADAR antidiscriminatiebureau
Bachelor scriptie HBO-Rechten

Auteur: Amy van de Klundert
Studentnummer: 2081480
Opdrachtgever: RADAR antidiscriminatiebureau, Spoorlaan 432, 5038 CX Tilburg
Stagementor: Mevrouw A. van Ravenstein
Opleidingsinstituut: Juridische Hogeschool Avans-Fontys, te Tilburg
1e stagedocent: Mevrouw mr. M.M.J. van den Haspel
2e stagedocent: De heer mr. J.D. Wesseling
Plaats en datum: Tilburg, 9 januari 2018

Voorwoord

Voor de afronding van mijn opleiding HBO-Rechten, heb ik de mogelijkheid gekregen om te mogen afstuderen bij RADAR antidiscriminatiebureau te Tilburg. Er is onderzoek gedaan naar het privacyrecht dat met de invoering van de AVG flink is aangescherpt. De vraag die centraal staat binnen dit onderzoek luidt als volgt;

'Welke aanbevelingen kunnen worden gegeven om het algemene privacybeleid en de werkwijze met betrekking tot de verwerking van persoonsgegevens van RADAR team klachtbehandeling zo aan te passen dat het privacybeleid en de werkwijze voldoen aan de Algemene verordening gegevensbescherming (AVG)?'

Ik wil graag mijn stagementor mevrouw Van Ravenstein bedanken voor alle hulp en inzet die zij mij heeft geboden gedurende de afstudeerperiode. Tevens wil ik graag mijn stagedocent mevrouw Van de Haspel bedanken voor haar begeleiding en feedback gedurende mijn afstudeertraject. De heer Wesseling wil ik ook graag bedanken voor de input die hij heeft geleverd bij het opstellen van mijn onderzoeksplan en voor het uitlenen van een literatuurboek. Verder wil ik alle collega's binnen RADAR bedanken voor hun collegialiteit. Tenslotte wil ik de organisatie RADAR bedanken voor het aanbieden van de afstudeerstage.

Veel leesplezier!

Amy van de Klundert

Tilburg, 9 januari 2018

Inhoudsopgave

Samenvatting

RADAR is een laagdrempelige voorziening die bijstand verleent aan personen die worden gediscrimineerd op diverse gronden. Naast het verlenen van bijstand, dient RADAR ook de klachten te registreren. De Wet Gemeentelijke Antidiscriminatievoorzieningen is sinds 2009 van kracht en reguleert klachtbehandeling en registratie van meldingen. De klachten worden binnen RADAR behandeld door de medewerkers in team klachtbehandeling. De klachtbehandelaars zijn verdeeld over de regio's: Rotterdam-Rijnmond, Midden- en West-Brabant en Zuidoost-Brabant. Enkele klachtbehandelaars werken voor meerdere regio's. De klachtbehandelaars registeren de klachten met inachtneming van de Wet Bescherming Persoonsgegevens. Vanaf mei 2018 is er een nieuw wettelijk kader voor het verwerken van persoonsgegevens binnen de gehele Europese Unie van toepassing. De Algemene verordening gegevensbescherming zal op 25 mei 2018 van kracht zijn. Binnen RADAR is echter weinig kennis over de privacywetgeving waardoor het noodzakelijk is om een onderzoek te verrichten naar de plichten die de Algemene verordening gegevensbescherming aan RADAR stelt. Dit onderzoek zal RADAR de nodige handvaten bieden om de gegevensverwerking op één lijn te brengen met de wettelijke eisen. Om RADAR een opzet te geven, is er een aanvulling gegeven op het privacybeleid. Daarnaast is er een nieuwe tekst ontwikkeld om op de website te plaatsen en er is een stappenplan opgesteld om de klachtbehandelaars bewust te maken van de privacy van cliënten.

In dit onderzoeksrapport wordt duidelijk op welke wijze klachten worden ingediend en worden geregistreerd. Allereerst wordt het privacybeleid en de website, gelet op informatieverstrekking, inhoudelijk geanalyseerd. Vervolgens wordt de werkwijze in de praktijk uiteengezet. Hiervoor hebben verschillende observaties en gesprekken plaatsgevonden. Daarnaast is het juridisch kader, gelet op noodzakelijk bepalingen voor dit onderzoek uit de Algemene Verordening Gegevensbescherming, beschreven. De verwerking van deze persoonsgegevens dient op een zorgvuldige wijze conform de privacywetgeving te gebeuren. Verder worden het privacybeleid en de huidige werkwijze getoetst aan de Algemene Verordening Gegevensbescherming. Tot slot worden er conclusies en aanbevelingen gegeven die van belang zijn voor RADAR.

Uit onderzoek blijkt dat verschillende bepalingen uit de Algemene Verordening Gegevensbescherming, niet voldoende worden nageleefd door RADAR. De organisatie heeft een privacybeleid, maar heeft deze enkel intern uitgezet. Cliënten van RADAR hebben hierdoor geen kennis van de rechten en plichten die zij toekomen. Op dit moment vraagt RADAR geen toestemming voor het verwerken van bijzondere persoonsgegevens van cliënten. Wanneer er contact met de cliënt wordt opgenomen om te bemiddelen, dient RADAR toestemming te vragen om de persoonsgegevens te verstrekken aan de wederpartij. Ook blijkt in de praktijk dat klachtbehandelaars geen eenduidige werkwijze hebben met het verwerken van de persoonsgegevens in het bijbehorend registratiesysteem. Hierdoor worden er meer gegevens verwerkt van cliënten dan noodzakelijk. Gegevens worden verwerkt in een landelijk registratiesysteem dat door bijna alle discriminatievoorzieningen wordt gebruikt. Er is gebleken dat met de maker van het systeem, de verwerker, geen verwerkersovereenkomst is opgesteld. Door zowel RADAR als de verwerker zijn geen instructies opgesteld hoe de medewerkers om dienen te gaan met een datalek.

Door de inwerkingtreding van de Algemene Verordening Gegevensbescherming komt er een aantal nieuwe verplichtingen bij voor RADAR. De organisatie moet kunnen aantonen dat zij voldoen aan de documentatieplicht. De informatieplicht naar betrokkenen toe is enorm uitgebreid. Daarnaast blijkt uit het onderzoek dat de organisatie verplicht is om een gegevensbeschermingseffectbeoordeling uit te voeren. Privacyrisico's worden hierdoor aan het licht gebracht. Er worden in dit onderzoek verschillende aanbevelingen gegeven. Deze aanbevelingen kunnen ervoor zorgen dat RADAR zich kan houden aan de wettelijke eisen voor de gegevenswerking gelet op Algemene Verordening Gegevensbescherming.

De belangrijkste aanbeveling voor RADAR is, het toestemming vragen voor het verwerken van bijzondere persoonsgegevens aan cliënten. Andere belangrijke aanbevelingen zijn: de beveiliging van de verwerking nóg veiliger te maken door de registratiesystemen zo in te richten dat ze minimaal gegevens verwerken, een functionaris voor de gegevensbescherming aan te stellen, een gegevensbeschermingsbeleid op te stellen of hervormen van het privacybeleid en tot slot de medewerkers bewust laten worden van de risico’s die de verwerking van persoonsgegevens met zich mee brengen.

Lijst van afkortingen

ADV	Antidiscriminiatievoorzieningen
AP	Autoriteit Persoonsgegevens
APV	Algemene plaatselijke verordening
Art.	Artikel
ART 1.	Artikel 1
AVG	Algemene verordening gegevensbescherming
BW	Burgerlijk wetboek
CBP	College Bescherming Persoonsgegevens
CVRM	College Voor de Rechten van een Mens
DPIA	Data Privacy Impact Assessment
EVRM	Europees Verdrag voor de Rechten van de Mens
FG	Functionaris Gegevensbescherming
GW	Grondwet
jo.	Juncto
LvtD	Landelijke vereniging tegen Discriminatie
MvT	Memorie van toelichting
Wbp	Wet bescherming persoonsgegevens
WGA	Wet Gemeentelijke Antidiscriminatievoorzieningen
Wmd	Wet meldplicht datalekken

Begrippenlijst

Persoonsgegevens: Onder persoonsgegevens kan worden verstaan: ‘elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon’. Indien een gegeven direct of indirect herleidbaar is naar een natuurlijk persoon, kan dit als een persoonsgegeven worden gezien. Er bestaan twee categorieën persoonsgegevens. De reguliere persoonsgegevens en de bijzondere persoonsgegevens. Bij reguliere persoonsgegevens kun je denken aan voor de hand liggende gegevens zoals namen, adressen, woonplaatsen of telefoonnummers. [1] Bijzondere persoonsgegevens zijn bijvoorbeeld gegevens over het ras, de godsdienst, gezondheid of seksuele voorkeur. Er worden strengere eisen gesteld aan de verwerking van bijzondere persoonsgegevens. Bijzondere persoonsgegevens worden in de AVG beschreven als ´bijzondere categorieën van persoonsgegevens´. Genetische gegevens, zoals DNA-gegevens, en biometrische gegevens, zoals vingerafdrukken, vallen nu ook onder ´bijzondere categorieën van persoonsgegevens´.[2]
Verwerking: Het begrip verwerking heeft betrekking op het algehele proces dat persoonsgegevens doormaken. Het proces begint bij het verzamelen van gegevens en eindigt bij de vernietiging van de gegevens. Het verzamelen, vastleggen, ordenen, bewaren, bewerken, wijzigen, opvragen, raadplegen en gebruiken van persoonsgegevens wordt allemaal beschouwd als de verwerking van persoonsgegevens.[3]
Bestand: Bestand wordt gedefinieerd als: ‘Elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen.’ Het begrip bestand is alleen van belang om te bepalen of niet-geautomatiseerde verwerking binnen de kaders van de AVG valt.[4]
Verwerkingsverantwoordelijke: De verantwoordelijke gedefinieerd als: ’de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.’ De verantwoordelijke is kortom de natuurlijke persoon of rechtspersoon onder wiens verantwoordelijkheid de gegevensverwerking plaatsvindt. Kortom de verwerkingsverantwoordelijke bepaalt het doel en de middelen voor het gebruik van persoonsgegevens.[5]
Verwerker: De verwerker wordt omschreven als degene die ‘in opdracht van’ de verantwoordelijke persoonsgegevens verwerkt, maar zonder aan zijn rechtstreekse gezag verbonden te zijn.

[1] J. Berkvens & C. Jakimowicz, Tekstuitgave Privacyverordening met geïntegreerde overwegingen, Wbp- en Richtlijn 95/46/EG-teksten en verwijstabellen, Den Haag: Boom juridisch 2016, p. 23
[2] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 31.
[3] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 22.
[4] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 25.
[5] Mr. L.H. von Meijenfeldt, *De AVG en Awb: vragen over babylonische spraakverwarring,* p. 124.

In de praktijk kiezen de verwerkers zelf de middelen waarmee zij werken, zoals de te gebruiken software of de wijze van archiveren van documenten. [6]
Betrokkene/ontvanger: De betrokkene of ontvanger is een natuurlijke persoon of rechtspersoon, al dan niet een derde, van wie de persoonsgegevens worden verwerkt.[7]
Toestemming: De verwerkingsverantwoordelijke moet in veel gevallen kunnen aantonen dat er toestemming is verleend om de gegevens van betrokkene te verwerken. De betrokkene moet goed geïnformeerd worden en instemmen met de verwerking van zijn of haar persoonsgegevens. Deze instemming moet gegeven zijn door een actieve handeling van de betrokkene.[8]
Pseudonimisering: In de AVG wordt een nieuw begrip geïntroduceerd, namelijk: 'pseudonimisering'. De persoonsgegevens zoals naam, adres of BSN worden bij verwerking geheel vervangen door een code. Deze code zou dan niet meer te herleiden moeten zijn tot de oorspronkelijke gegevens.[9] De gegevensbeschermingsbeginselen zijn niet meer van toepassing op anonieme gegevens. Anonieme gegevens worden gezien als gegevens die geen betrekking hebben op een geïdentificeerde of identificeerbare natuurlijk persoon, of persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet of niet meer identificeerbaar is. Een nummer of code zegt namelijk minder over een identificeerbaar persoon dan de persoonsgegevens zelf. [10]

[6] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 26.
[7] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 27.
[8] J. Berkvens & C. Jakimowicz, Tekstuitgave Privacyverordening met geïntegreerde overwegingen, Wbp- en Richtlijn 95/46/EG-teksten en verwijstabellen, Den Haag: Boom juridisch 2016, p. 25.
[9] 'Privacy by design', Privacy, www.justitia.nl/ (zoek op *privacy by design*).
[10] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 15.

1. Inleiding

In dit hoofdstuk zal de afbakening van het onderzoek worden weergegeven. Allereerst zal er een beschrijving van de organisatie worden gegeven. Hierna zal de probleembeschrijving toegelicht worden. Aan de hand van de probleembeschrijving zal de centrale vraag, de deelvragen en de doelstelling worden geformuleerd. Verder zullen de onderzoeksmethoden van de betreffende deelvragen worden beschreven. Tot slot volgt de leeswijzer van dit onderzoek.

§ 1.1 De afstudeerorganisatie

RADAR antidiscriminatiebureau is een stichting die in 1983 is opgericht als een Rotterdamse onderzoeksinstelling op het gebied van rassendiscriminatie. RADAR Inc., corporate is het moederbedrijf die verschillende holdings onder zich heeft. Het moederbedrijf is in eerste instantie opgericht door de raad van bestuur. RADAR Inc. bevat meerdere werkmaatschappijen. De werkmaatschappijen van RADAR Inc. zijn RADAR en Art.1 en IDEM. Deze werkmaatschappijen hebben verschillende werkzaamheden. IDEM houdt zich bezig met projecten die zich voordoen in specifiek Rotterdam. Zij werken vanuit vier thema's en zetten zich in voor nieuwe ontwikkelingen die zij vormgeven in Rotterdam. De andere werkmaatschappij betreffen stichting RADAR en Art. 1. Deze werkmaatschappijen zijn met elkaar gefuseerd. Zo houdt Art.1 zich bezig met onderzoek en houdt RADAR zich voornamelijk bezig met preventie, het voorkomen en bestrijden van discriminatie en klachtbehandeling.

Dit onderzoek zal plaatsvinden bij Stichting RADAR, specifiek team klachtbehandeling. RADAR vervult de functie van meldpunt voor klachten voor ongeveer 60 gemeentes. Vanaf februari 1985 is een meldpuntfunctie onderdeel gaan uitmaken van RADAR. Meer mensen konden door de meldpuntfunctie met hun klachten over discriminatie op grond van ras, religie/levensovertuiging, sekse, seksuele gerichtheid, handicap/chronische ziekte en leeftijd en alle overige gronden terecht bij het meldpunt van RADAR. Team klachtbehandeling kan zaken waarin het vermoeden bestaat dat er sprake is van discriminatie in uiterste geval voorleggen aan het College voor de Rechten van een Mens (hierna: CVRM). De klachtbehandelaar zal in eerste instantie in voorkomende gevallen hoor en wederhoor toepassen. In sommige zaken leidt dit tot een gesprek en de klachtbehandelaar bemiddelt hier tussen de melder en de tegenpartij. Mocht dit bemiddelingsgesprek niet baten, kan RADAR zaken voorleggen aan het CVRM. Het College bekijkt op basis van de Algemene Wet Gelijke Behandeling of er daadwerkelijk sprake is van discriminatie en beoordeelt de zaak.[11]

§ 1.2 De probleembeschrijving

Iedere gemeente is wettelijk verplicht om een laagdrempelige onafhankelijke voorziening in te stellen, waar burgers terecht kunnen met klachten over discriminatie.[12] In de gebieden Brabant-Noord locatie 's-Hertogenbosch, Zuidoost-Brabant locaties Den Bosch en Eindhoven, Midden- en West-Brabant locatie Tilburg, Rotterdam-Rijnmond en Zuid-Holland-Zuid locatie Rotterdam, vormt RADAR één gezamenlijk onafhankelijk antidiscriminatiebureau.[13] Stichting RADAR antidiscriminatiebureau zet zich in voor mensen die zich niet gelijk behandeld voelen. In artikel 1 (hierna: art.) van onze grondwet wordt ook duidelijk gezegd dat: *''Allen die zich in Nederland bevinden, worden in gelijke gevallen gelijk behandeld. Discriminatie wegens godsdienst, levensovertuiging, politieke gezindheid, ras, geslacht of op welke grond dan ook, is niet toegestaan''*.

[11] 'Oordelen CRM', Read, www.radar.nl (zoek op *oordelen CRM*).
[12] Artikel 2, Wet gemeentelijke antidiscriminatievoorzieningen
[13] 'Discriminatiemeldpunt RADAR, Praktijkvoorbeeld, www.databank-antidiscriminatie.nl (zoek op *discriminatiemeldpunt RADAR*).

Indien mensen zich niet gelijk behandeld voelen op grond van religie/levensovertuiging, sekse, seksuele gerichtheid, handicap/chronische ziekte, leeftijd of een andere grond, kunnen zij een klacht indienen bij de klachtbehandeling van RADAR.[14] Op alle locaties bestaat er een mogelijkheid om tijdens kantooruren het kantoor te bezoeken en fysiek een klacht in te dienen. Er wordt op dit moment meer gebruik gemaakt van digitale middelen. Dit wordt door de medewerkers van RADAR gestimuleerd. Er kan online via de website van RADAR een klachtenformulier worden ingevuld. Via discriminatie.nl worden klachten naar de juiste regio's geleid. Ook kunnen er klachten telefonisch, via e-mail, WhatsApp of Facebook worden ingediend. Alle klachten en gegevens van de melder worden vastgelegd in het klachtenregistratiesysteem van RADAR, dit wordt 'LBA-net' genoemd. RADAR is aangesloten bij een Landelijke Brancheorganisaties Antidiscriminatiebureaus. Vrijwel alle aangesloten discriminatiesbureaus maken gebruik van dit landelijke systeem LBA-net. Dit landelijke systeem is gebouwd door een ICT-bedrijf genaamd 'Constant IT'. RADAR heeft bij team onderzoek een contactpersoon die samen met Constant IT het registratiesysteem beheert. Daarnaast laat RADAR door een extern ICT-bedrijf 'Trends' de overige automatisering regelen. In de wet wordt het registeren van persoonsgegevens in een registratiesysteem, 'het verwerken van persoonsgegevens genoemd'. RADAR verwerkt vooral veel privacygevoelige gegevens en veelal betreffen dit ook bijzondere persoonsgegevens. Persoonsgegevens zijn bijzonder als deze bijvoorbeeld een geloofsovertuiging of politieke voorkeur aanduiden.[15] Tijdens de verwerking van bijzondere gegevens dient de verwerker zich aan nog striktere regels te houden.

Met ingang van 25 mei 2018 is de Algemene verordening gegevensbescherming (hierna: AVG), (Verordening (EU) 2016/679) van toepassing en wordt de Richtlijn 95/46/EG (algemene verordening gegevensbescherming) ingetrokken.[16] De Wbp verdwijnt door deze verandering uit het Nederlandse wetboek. Hier is een internationale wetgeving voor in de plaats gekomen, namelijk de AVG. Als de AVG van toepassing is, geldt er nog maar één privacywet in de hele Europese Unie in plaats van 28 verschillende nationale wetten. Dit feit brengt wel een aantal veranderingen voor organisaties met zich mee. Door het in werking treden van de AVG wordt er bij bedrijven de nadruk gelegd op de verantwoordelijkheid van bedrijven zelf dat zij zich aan de wet houden.[17] Door het in werking treden van de AVG zullen er meer rechten aan de betrokkene worden toegekend. Zo heeft een betrokkene onder andere het recht om te weten hoelang de gegevens worden bewaard en wie de ontvangers zijn van de persoonsgegevens.[18]

Naar aanleiding van de vastgestelde AVG wil RADAR weten welke gevolgen dit met zich meebrengt voor de organisatie. De opdrachtgever, meer gespecificeerd de directeur van RADAR Inc., vraagt zich met name af of de privacywet wel correct wordt toegepast in de praktijk. In de praktijk is er namelijk een verouderd privacybeleid (2009) op de gezamenlijke SharePoint van RADAR gedeeld. Vanuit dit privacybeleid is er een werkwijze protocol klachtbehandeling opgesteld. Daarnaast gebruikt RADAR een registratiesysteem waarin de gegevensverwerking wordt gedaan. Gelet op enkele bepalingen uit de AVG, bijvoorbeeld 'dataminimalisatie' wordt het huidige registratiesysteem onder de loep genomen en naar aanleiding daarvan worden er aanbevelingen gegeven aan de organisatie voor het nieuwe registratiesysteem. In januari 2018 wordt er een nieuw registratiesysteem gelanceerd, dus hierdoor is het erg van belang dat deze AVG-proof wordt gemaakt.

[14] 'Discriminatie factsheets', Read, www.radar.nl (zoek op *discriminatie factsheets*).
[15] 'Wat zijn persoonsgegevens', Over Privacy, Persoonsgegevens, www.autoriteitpersoonsgegevens.nl/ (zoek op *wat zijn persoonsgegevens*).
[16] D.E. Comijs , P&I 2016/253, afl. 6, p. 250-257.
[17] 'Algemene verordening gegevensbescherming', Autoriteit persoonsgegevens 2017, www. autoriteitpersoonsgegevens.nl (zoek op *Algemene verordening gegevensbescherming*).
[18] Mr. E. Oude Elferink & Mr. J.G. Reus, NtEr 2017, afl. 6, p. 157-159.

RADAR is op de hoogte van de boetes die de Autoriteit Persoonsgegevens (hierna: AP), kan opleggen indien de regels van de AVG niet worden nageleefd.[19] In dit onderzoek wordt er alleen ingegaan op de verwerking van de gegevens van cliënten en niet op gegevensverwerking van eigen medewerkers. De klachtbehandeling werkt voornamelijk extern. Wegens het feit dat de rechten van betrokkenen in de AVG enorm zijn aangescherpt, wordt in dit onderzoek hierop de nadruk gelegd. Het privacybeleid en de manier van informatieverstrekking aan cliënten door middel van de website en de werkwijze in de praktijk worden geanalyseerd. Er wordt uiteengezet wat de praktische consequenties van de inwerkingtreding van de AVG zijn voor de werkwijze omtrent gegevenswerking en welke aanbevelingen te geven zijn om de werkwijze zodanig aan te passen dat deze conform de AVG is. Tot slot wordt er voor de organisatie een aanvulling gedaan op privacybeleid en een aanvulling gegeven op de privacy statement die te vinden is op de website van RADAR.

§ 1.3 De doelstelling

Het doel is om vóór 9 januari 2018 een onderzoeksrapport aan Cyriel Triesscheijn, de directeur van RADAR antidiscriminatiebureau, te overhandigen waarin aanbevolen wordt hoe de huidige werkwijze van team klachtbehandeling met betrekking tot het verwerken van persoonsgegevens moeten worden aangepast om in overeenstemming te komen met de AVG. Daarnaast wordt er een aanvulling gedaan op het huidige privacybeleid, manier van informatieverstrekking en worden de directeur en klachtbehandelaars geïnformeerd over hoe de gegevens verwerkt kunnen worden om aan de vereisten van de AVG te voldoen.

§ 1.4 De centrale vraag

'Welke aanbevelingen kunnen worden gegeven om het algemene privacybeleid en de werkwijze met betrekking tot de verwerking van persoonsgegevens van RADAR team klachtbehandeling zo aan te passen dat het privacybeleid en de werkwijze voldoen aan de Algemene verordening gegevensbescherming (AVG)?'

§ 1.5 De deelvragen

1. Hoe luidt het huidige privacybeleid en op welke manier wordt er informatie verstrekt door RADAR aan cliënten met betrekking tot het verwerken van persoonsgegevens ten aanzien van de klachtbehandeling?
2. Wat is de huidige werkwijze binnen RADAR met betrekking tot het verwerken van persoonsgegevens ten aanzien van de klachtbehandeling?
3. Welke eisen uit de relevante wet -en regelgeving zijn van toepassing op de verwerking van persoonsgegevens en wat zijn de wijzigingen die de AVG met zich meebrengt?
4. In welke mate dient het algemene privacybeleid, de manier van informatieverstrekking aan cliënten en de werkwijze van RADAR team klachtbehandeling te worden aangepast om aan de toekomstige wet- en regelgeving (AVG) te voldoen?

§ 1.6. De afbakening

Om de relevante wet- en regelgeving te beschrijven, zijn bepalingen uit de huidige Wbp kort opgesomd en vervolgens aangevuld met de eisen die de AVG met zich meebrengt. Het praktijkonderzoek beperkt zich tot de gegevensverwerking van cliënten. Interne gegevensverwerkingen over personeel worden buiten beschouwing gelaten. De gegevensverwerking in de praktijk, het privacybeleid en de wijze van informatieverstrekking wordt uitsluitend getoetst aan de AVG. De Wbp en de Richtlijn 95/46 zijn tijdens de toetsing buiten beeld gelaten.

[19] 'Algemene informatie AVG, Onderwerpen, AVG nieuwe Europese privacywetgeving, www.autoriteitpersoonsgegevens.nl/ (zoek op *Algemene informatie AVG*).

§ 1.7 De methoden en verantwoording van het onderzoek

Deelvraag 1:

'Hoe luidt het huidige privacybeleid en op welke manier wordt er informatie verstrekt door RADAR aan cliënten met betrekking tot het verwerken van persoonsgegevens ten aanzien van de klachtbehandeling?'

Voor beantwoording van deze deelvraag is gebruik gemaakt van documentenanalyse.
Er is gebruik gemaakt van verschillende documenten behorend tot de organisatie zoals het privacybeleid, het klachtformulier, de website, werkinstructies en protocollen.
Deze documenten zijn vervolgens geanalyseerd en uiteengezet. RADAR heeft een gezamenlijke SharePoint waar alle protocollen en werkinstructies te vinden zijn. Daarnaast heeft RADAR op de algemene website een privacyclausule geplaatst.[20] Dit wordt de wijze van informatieverstrekking genoemd.

Deelvraag 2:

'Wat is de huidige werkwijze binnen RADAR met betrekking tot het verwerken van persoonsgegevens ten aanzien van de klachtbehandeling?'

Om concrete aanbevelingen te kunnen geven aan RADAR is het noodzakelijk om de werkwijze gegevensverwerking van team klachtbehandeling grondig te analyseren. Er wordt hier gebruik gemaakt van een veldonderzoek aangevuld met een casestudy. In dit veldonderzoek worden er verschillende observaties met aanvullende gesprekken gevoerd. De observatie/gesprekken worden verwerkt in observatie- en gespreksverslagen waarin ook staat aangegeven wat de observant heeft medegedeeld gedurende de observaties. Deze informatie is vervolgens in een observatie- en gespreksverslag verwerkt. Het landelijke protocol klachtbehandeling is als leidraad gebruikt bij de observaties. Er zijn drie personen van team klachtbehandeling geobserveerd om de werkwijze in beeld te krijgen. Er is gekozen voor drie personen, omdat er één klachtbehandelaar van elke regio wordt geobserveerd. Eén klachtbehandelaar is actief in twee regio's en daarom is de observatie beperkt gehouden tot drie personen. Daarnaast wordt er bij het in kaart brengen van de praktijk ook het registratiesysteem bekeken. Het registratiesysteem is een landelijk systeem genaamd LBA-net. Alle aangesloten leden van de Landelijke Brancheorganisaties Antidiscriminatiebureaus krijgen begin 2018 een nieuw registratiesysteem. LBA-net wordt vervangen door een geheel nieuw systeem. Het registratiesysteem is van essentieel belang want in dit programma worden de klachten geregistreerd. Er is een medewerker van de werkgroep van RADAR team onderzoek geïnterviewd. Voorafgaand aan het interview is de vragenlijst opgestuurd. Tijdens het interview heeft de medewerker de vragenlijst persoonlijk beantwoord.[21] In dit interview wordt duidelijk of bij het ontwerpen van een nieuw registratiesysteem de regels van de AVG zijn meegenomen. Na het interview is er een training gegeven over het nieuwe systeem 'ADV-net' voor alle medewerkers van de landelijke antidiscriminatiebureaus. De bronnen voor het beantwoorden van deze deelvraag zijn dan ook het registratiesysteem, het klachtenprotocol en de geïnterviewde/geobserveerde personen.

Deelvraag 3:

'Welke eisen uit de relevante wet -en regelgeving zijn van toepassing op de verwerking van persoonsgegevens en wat zijn de wijzigingen die de AVG met zich meebrengt?'

In dit hoofdstuk zal een grondige inhoudsanalyse van het recht worden weergegeven. De onderzoekstrategie die hier is toegepast is een rechtsbronnen- en literatuuronderzoek. De voorwaarden van de verscheidene wetten, zoals bruikbare delen uit de Wbp en de AVG, zullen hier gestructureerd worden weergegeven. Er is gebruikgemaakt van de delen uit de Wbp om het huidige recht uit een te zetten.

[20] Uw privacy, RADAR, www.radar.nl (zoek op *uw privacy*).
[21] Cursus interviewtechnieken, 22 september 2017.

Hoofdzakelijk zijn de bepalingen uit de AVG die bruikbaar zijn voor dit onderzoek uiteengezet. Verschillende betrouwbare internetsites zijn geraadpleegd. De website van de Autoriteit Persoonsgegevens en Privacycompany spelen daarbij een grote rol. Daarnaast zijn vaktijdschriften o.a. Privacy en Informatie van uitgeverij Paris geraadpleegd, die te vinden zijn in de mediatheek op de Juridische Hogeschool of in de Xplora databank. Het literatuurboek ICT-recht 'De Algemene Verordening Gegevensbescherming' van Engelfriet, Chew-Meij en Kager is ook veelvuldig geraadpleegd. Er is gebruikgemaakt van verschillende jurisprudentie en de Uitvoeringswet van de AVG.
Het juridisch kader moet bekend zijn alvorens er kan worden overgegaan naar een analyse of de werkwijze in overeenstemming is met de AVG.

Deelvraag 4:
'In welke mate dient het algemene privacybeleid, de manier van informatieverstrekking aan cliënten en de werkwijze van RADAR team klachtbehandeling te worden aangepast om aan de toekomstige wet- en regelgeving (AVG) te voldoen?'

Bij het beantwoorden van deze deelvraag is de praktijk toegepast op het recht. De methode die is toegepast bij deze deelvraag zal een inhoudsanalyse, meer gericht een documentenonderzoek zijn. De selectie van de relevante bepalingen die vanuit de WBP blijven bestaan en/of worden aangevuld door de AVG vormen het beoordelingskader voor deze toetsende deelvraag. In deze deelvraag wordt de gehele praktijk getoetst aan de AVG. Dit houdt in dat het privacybeleid, de website en de werkwijze gegevensverwerking van team klachtbehandeling aan de regels van de AVG worden getoetst. De toetsing vormt het belangrijkste onderdeel voor het beantwoorden van de centrale vraag. Naar aanleiding van deze toetsing kan immers worden geconcludeerd in hoeverre de werkwijze in overeenstemming is met de AVG. De relevante bepalingen uit de Wbp/AVG, de observaties, de gesprekken, het interview en de overige bijlagen zijn als bronnen gebruikt om deze deelvraag te beantwoorden. De nieuwe verplichtingen uit de AVG worden tevens getoetst in deze deelvraag.

§ 1.8 De leeswijzer

In hoofdstuk twee zal worden ingegaan op de praktijkgerichte werkwijze van de organisatie. Het algemene privacybeleid en de privacyclausule op de site worden in dit hoofdstuk beschreven. In hoofdstuk drie zal de praktijkgerichte werkwijze door de klachtbehandelaars uiteen worden gezet. Bij het beantwoorden van deze deelvraag was het nodig om het veld in te gaan. Enkele medewerkers van team klachtbehandeling zijn geobserveerd en er zijn aanvullende vragen gesteld. Er heeft een interview plaatsgevonden met een medewerker van RADAR gelet op het registratiesysteem. In hoofdstuk vier zal het juridische kader voor de toepassing op de verwerking van persoonsgegevens uiteengezet worden. Hierbij worden de WBP en AVG beide beschreven. De wijzigingen van de AVG ten opzichte van de Wbp worden in dit hoofdstuk kort beschreven. Dit hoofdstuk zal zich voornamelijk richten op de relevante bepalingen uit de AVG. Vervolgens wordt in hoofdstuk vijf beschreven in welke mate het privacybeleid, de informatieverstrekking op de website en de gegevensverwerking in de praktijk door de klachtbehandelaars voldoen aan de AVG. Er wordt in dit hoofdstuk een grondige inhoudsanalyse gemaakt van de praktijk en de toekomstige wet- en regelgeving waaraan voldaan moet worden. De tekortkomingen en knelpunten van de huidige werkwijze worden uiteengezet in dit hoofdstuk. In hoofdstuk zes zullen de conclusies en aanbevelingen komen te staan. Hier zal aan de hand van de conclusies antwoord gegeven worden op de centrale vraag. De aanbevelingen worden samengevat in dit hoofdstuk. Tot slot zal in hoofdstuk acht de literatuurlijst opgenomen worden.

2. Huidig privacybeleid en privacyclausule website

In dit hoofdstuk wordt allereerst de structuur van RADAR besproken. Er wordt duidelijk gemaakt op welke wijze RADAR is opgericht. Vervolgens wordt er een korte uitleg gegeven over team klachtbehandeling en wat het verband is met dit onderzoek. In paragraaf 2.1.1 wordt duidelijk gemaakt wie de verwerkingsverantwoordelijke en de verwerkers zijn. Verder wordt het huidige privacybeleid van RADAR uiteengezet. Het privacybeleid bestaat uit verschillende passages die zijn opgenomen in meerdere documenten die voor de gehele organisatie gelden. Tot slot is er beschreven op welke manier informatie wordt verstrekt, voordat er een klacht wordt ingediend door de betrokkene. Hiervoor wordt gebruik gemaakt van een privacyclausule op de website.

§ 2.1 Structuur RADAR

De volgende regio's zijn samen werkzaam onder RADAR: Rotterdam-Rijnmond, Midden- en West-Brabant, Brabant-Noord, Zuidoost-Brabant en Zuid-Holland-Zuid. De WGA reguleert de instelling en werkwijze van gemeentelijke antidiscriminatievoorzieningen. Deze wetgeving bepaalt dat het verplicht is dat eenieder toegang heeft tot een laagdrempelige gemeentelijke voorziening die de behandeling en registratie van klachten over discriminatie op zich neemt. In art. 2 Wet gemeentelijke antidiscriminatievoorzieningen staat dat antidiscriminatievoorzieningen de taak heeft om onafhankelijke bijstand te verlenen. Zij moeten personen bijstand verlenen bij de afwikkeling van hun klachten gelet op onderscheid (discriminatie) op grond van de gelijkebehandelingswetgeving. In lid 2 van dit artikel staat dat de discriminatieklachten geregistreerd moeten worden.[22]

Stichting RADAR is opgericht door directeur/bestuurder Cyriel Triesschijn. Cyriel Triesschijn geeft leiding aan stichting RADAR en Radar Inc.[23] Hij heeft de eindverantwoordelijkheid voor de totaliteit van de organisatie (Radar Inc.). RADAR bestaat uit team klachtbehandeling, preventie en onderzoek. Dit onderzoek zal zich alleen richten op de verwerking van persoonsgegevens door team klachtbehandeling.

Team klachtbehandeling van RADAR bestaat feitelijk uit acht klachtbehandelaars waarvan er één momenteel niet actief is. De klachtbehandelaars werken per regio waarvan er twee in alle regio's werkzaam zijn. De standplaatsen van de klachtbehandelaars zijn verdeeld onder: Rotterdam, Tilburg en 's-Hertogenbosch. En sinds 1 januari 2018 Eindhoven.

§ 2.1.1 Verwerkingsverantwoordelijke/verwerker

In paragraaf 2.1 is duidelijk geworden dat Cyriel Triesschijn de directeur/bestuurder is. De directeur/bestuurder is de verwerkingsverantwoordelijke voor alle verwerkingen rondom persoonsgegevens. Hij bepaalt formeel-juridisch wat het doel en de middelen zijn die worden vastgesteld voor de verwerking van persoonsgegevens.[24] Hierdoor kan hij, en dus RADAR worden aangemerkt als de verwerkingsverantwoordelijke.[25] Verder kunnen de externe ICT-bedrijven, die RADAR heeft aangesteld, worden aangemerkt als 'verwerker'. Zij verwerken ten behoeve van de verwerkingsverantwoordelijke de persoonsgegevens. Zij hebben ook de taak om de persoonsgegevens te beveiligen. Er bestaat ook een geheimhoudingsplicht met de verwerker en deze moet uitsluitend in opdracht van de verantwoordelijke persoonsgegevens verwerken.[26] Op dit moment is Constant-IT de verwerker van RADAR. Constant-IT heeft het huidige registratiesysteem ontwikkeld en momenteel in beheer. Vanaf 1 januari 2018 beheert Enigmatry het registratiesysteem, de ontwikkeling van het systeem is ook in handen van Enigmatry.

---

[22] 'Over ons', Read, www.radar.nl (zoek op *Over ons*).
[23] 'Medewerkers', Read, www.radar.nl (zoek op *Medewerkers)*.
[24] Artikel 29 AVG.
[25] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 115.
[26] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 125.

Hierdoor kan Enigmatry vanaf januari 2018 aangemerkt worden als verwerker van de persoonsgegevens. Team klachtbehandeling opereert onder de verantwoordelijkheid en op aanwijzing van de verwerkingsverantwoordelijke. Dit betekent dat zij ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt, maar niet worden aangemerkt als verwerkers.[27] In de volgende paragrafen zullen essentiële onderdelen uit het privacybeleid met betrekking tot gegevensverwerking worden uitgelicht.

§ 2.2 Huidig privacybeleid

Het privacybeleid van RADAR is te vinden op de gezamenlijke SharePoint. De medewerkers kunnen de SharePoint bereiken door het webadres: www.portal.office.com. Deze kan ook geraadpleegd worden door de Windows verkenner op het bureaublad. Via de SharePoint kom je op de interne teamsite terecht. De teamsite bestaat uit verschillende mappen. In de map gemeenschappelijk kan bij handige info voor medewerker, in de map cao- en reglementen, het privacybeleid worden geraadpleegd. Dit beleid is alleen te raadplegen door de werknemers van RADAR. Het beleid wordt verder nergens gepubliceerd of verspreid. Het privacybeleid bestaat uit verschillende passages rondom privacy die in verschillende organisatiedocumenten zijn opgenomen. Hierbij kun je denken aan het personeelsreglement, het arbeidscontract, het protocol klachtbehandeling en de gedragscode omgaan met persoonsgegevens van klachtindieners.[28] Het protocol klachtbehandeling kan door cliënten worden geraadpleegd via de website van RADAR.[29] Enkele passages zijn geheel overgenomen uit het beleid, de overige passages zijn samengevat.

De volgende onderwerpen die worden aangehaald zijn terug te vinden in het volledige privacybeleid.[30]

§ 2.2.1 Dossiervorming

In het actuele personeelsreglement is opgenomen dat de medewerker zorg moet dragen voor privacygevoelige gegevens. De gegevens dienen op een vertrouwelijke wijze worden geadministreerd en gearchiveerd. Dezelfde passage is opgenomen in het arbeidscontract, stagecontract en/of vrijwilligerscontract van elke medewerker. In het protocol klachtbehandeling is opgenomen dat de cliënt wordt geïnformeerd over de wijze van dossiervorming en hoe met deze gegevens wordt omgegaan. In de gedragscode wordt de passage herhaald die in het arbeidscontract en personeelsreglement is opgenomen en verder zijn er geen nieuwe bepalingen omtrent dossiervorming toegevoegd.

§ 2.2.2 Het verrichten van mededelingen aan derden

In het personeelsreglement is opgenomen dat medewerkers geen mededelingen mogen doen aan derden. Deze bepaling is gericht op mededelingen die betrekking hebben op de behandeling van individuele of collectieve klachten. In overleg met de teamleider kan hiervan worden afgeweken als het noodzakelijk is voor de correcte en doelmatige behandeling van zaken. In het arbeidscontract is hieraan toegevoegd dat deze bepalingen ook gelden voor andere interne zaken die als vertrouwelijk moeten worden gekenmerkt. In het protocol klachtbehandeling is opgenomen dat de persoonsgegevens vertrouwelijk blijven. De cliënt wordt verteld dat deze nooit zonder zijn of haar persoonlijke toestemming beschikbaar worden gesteld aan derden. In de gedragscode is de passage over mededelingen aan derden uit het personeelsreglement en arbeidscontract herhaald.

§ 2.2.3 Inzage door derden

In het personeelsreglement staat opgenomen dat inzage in dossiers door derden alleen kan plaatsvinden na toestemming door de teamleider of medewerker klachtbehandeling.
In het arbeidscontract staat niets opgenomen over inzage door cliënten in zijn of haar persoonsgegevens.

---

[27] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 133-134.
[28] Zie bijlage I voor protocol klachtbehandeling.
[29] Protocol klachtbehandeling 2014, RADAR, www.radar.nl (zoek op *protocol klachtbehandeling*).
[30] Zie bijlage II voor privacybeleid, RADAR juni 2017.

In het protocol klachtbehandeling is enkel de bepaling opgenomen dat de cliënt inzage heeft in het eigen dossier. In de gedragscode staat een volledige bepaling opgenomen: '*Iedereen mag met redelijke tussenpozen vragen of, en zo ja welke persoonsgegevens ten aanzien van hem zijn verwerkt. Als de betrokkene ons buitensporig vaak met een dergelijk verzoek benadert, hoeft daaraan geen gehoor te gegeven te worden. Op een verzoek om inzage moet binnen vier weken geantwoord worden. Het antwoord moet schriftelijk zijn, tenzij een gewichtig belang van de betrokkene vergt dat je een andere vorm kiest, bijvoorbeeld mondeling. Een per e-mail verzonden antwoord is ook schriftelijk. Het antwoord moet in een begrijpelijke vorm bevatten:*

- *een volledig overzicht van de verwerkte gegevens van de betrokkene;*
- *een omschrijving van het doel of de doeleinden van de gegevensverwerking;*
- *de categorieën van gegevens waarop de verwerking betrekking heeft;*
- *de ontvangers of categorieën van ontvangers;*
- *alle beschikbare informatie over de herkomst van de gegevens.*'[31]

§ 2.2.4 Vertrouwelijkheid

In het personeelsreglement is opgenomen dat er zorgvuldig dient te worden omgegaan met wachtwoorden (ook voor computerprogramma's), telebankieren en dergelijke vertrouwelijke gegevens. In het arbeidscontract wordt genoemd dat de werknemer zorgvuldig en vertrouwelijk dient om te gaan met privacygevoelige gegevens. De privacygevoelige gegevens dienen ook op een vertrouwelijke wijzen te worden geadministreerd. Ook volgens het protocol klachtbehandeling moeten de persoonsgegevens vertrouwelijk blijven. In de gedragscode wordt de passage uit het personeelsreglement en arbeidscontract herhaald.

§ 2.2.5 Wet bescherming persoonsgegevens

In een aantal passages uit verschillende documenten wordt de Wet bescherming persoonsgegevens (Wbp) aangehaald. In het personeelsreglement en arbeidscontract wordt de term Wbp overigens niet genoemd. In het protocol klachtbehandeling wordt alleen benoemd dat RADAR gebonden is aan de Wbp. In de gedragscode wordt hier dieper op ingegaan. Er staat dat RADAR op grond van de Wbp alleen gegevens mag verzamelen met het uitdrukkelijke doel klachtbehandeling, registratie en monitoring. Ook staat er dat het toenmalige College Bescherming persoonsgegevens (CBP), de huidige Autoriteit Persoonsgegevens (AP), eisen heeft gesteld aan het inrichten van de gegevensverwerking. Eén van die eisen zou zijn dat er steeds moet worden nagegaan of het gebruik van persoonsgegevens noodzakelijk is voor het doel waarvoor de toestemming is verleend. Er wordt aangegeven dat een persoon wiens persoonsgegevens worden verwerkt, altijd moet kunnen nagaan wat er met die gegevens gebeurt. De Wbp bevat een regeling over informatieverstrekking aan de betrokkene. De informatieverstrekking aan de betrokkene moet in ieder geval omvatten voor welk doel of doeleinden de gegevens worden verzameld en verwerkt.

§ 2.2.6 Beveiliging

In het personeelsreglement zijn een aantal bepalingen opgenomen rondom beveiliging van dossiers. Fysieke dossiers moeten buiten kantoortijd in een afgesloten kluis worden bewaard. Indien een dossier meegenomen wordt naar huis of buiten de organisatie, moet er in principe kunnen worden volstaan met een kopie van de noodzakelijke gegevens. Ook dient er een kopie van de eerste pagina met contactgegevens op kantoor in de kluis achter te laten. Verder is er een bepaling opgenomen dat er thuis zorgvuldig met dossiers en dossiergegevens moet worden omgegaan. Dit houdt in dat het dossier op een veilige plek opgeborgen moet worden en dat het niet uit het oog mag worden verloren. In het arbeidscontract en protocol klachtbehandeling staat verder niets opgenomen over beveiliging.

[31] Zie bijlage II voor Privacybeleid 2017, gedragscode laatste pagina.

In de gedragscode is de volgende passage opgenomen:' *De Wbp verplicht ons om onze persoonsgegevensverwerking te beveiligen. We moeten passende technische en organisatorische maatregelen nemen om het verlies van gegevens of onrechtmatige verwerking tegen te gaan. Organisatorische maatregelen kunnen bijvoorbeeld inhouden dat maar een beperkt aantal personen toegang heeft tot uw computersysteem.*
De (technische en organisatorische) maatregelen die we nemen, moeten een passend beveiligingsniveau garanderen. Passende beveiliging betekent dat in de keuze voor de methode van beveiliging de volgende elementen moet meewegen:

- *de risico's van de verwerking en de aard van de te beschermen gegevens. Hoe gevoeliger de gegevens, hoe zwaarder de toegepaste beveiliging moet zijn. Zijn de gegevens minder gevoelig, dan hoef je niet steeds de zwaarst mogelijke beveiligingsmaatregelen nemen;*
- *je moet rekening houden met de stand van de techniek en de kosten van de maatregelen. Als de kosten van extra maatregelen uitzonderlijk hoog zijn ten opzichte van de toename in beveiligingsniveau, dan zijn die maatregelen niet passend en hoeft je ze dus niet te nemen. Je kunt echter tegen geringe kosten komen tot een beduidend veiliger systeem, dan moet je deze maatregelen zeker nemen. De beveiliging moet steeds adequaat zijn. Dat betekent ook dat je periodiek moet nagaan of het systeem aanpassing behoeft, bijvoorbeeld door technologische ontwikkelingen.'*[32]

§ 2.2.7 Kwaliteitseisen

Enkel in de gedragscode wordt het begrip kwaliteitseisen genoemd. In de andere documenten komt dit begrip niet voor. In de gedragscode staat vermeldt dat de Wbp een algemene norm bevat over kwaliteit. De gegevensverwerkingen moeten gelet op het doel waarvoor ze verwerkt worden minimaal voldaan aan: niet bovenmatig zijn, toereikend en ter zake dienend zijn. Ook moet er worden gezorgd dat er voldoende adequate gegevens verwerkt worden voor het doel. Verder mogen er geen gedetailleerde gegevens verwerkt worden die voor het doel niet noodzakelijk zijn. Vervolgens wordt er een stuk beschreven over hoe kwaliteitseisen in de praktijk toegepast moeten worden: '*Op basis van de privacywetgeving zijn de databestanden waar de klachtbehandelaars mee werken alleen voor hen toegankelijk. De monitormedewerkers hebben toegang tot de klachtgegevens, omdat zij hieruit de informatie controleren en verwerken. Verder is het zo georganiseerd dat medewerkers alleen toegang hebben tot de klachten en meldingen van de vestiging waar zij werkzaam zijn. Daarnaast wordt er aangehaald dat de klachtbehandelaars zich telkens moeten afvragen of het noemen van namen in bijvoorbeeld een overleg noodzakelijk is. Zorgvuldigheid speelt een belangrijke rol bij het omgaan met persoonsgegevens.*'[33]

§ 2.3 Privacyclausule (website)

RADAR heeft een algemene website waar zij informatie op delen.[34] Actuele uitspraken van het CVRM worden door de beheerders up-to-date gehouden. Het protocol klachtbehandeling en de klachtformulieren zijn tevens te raadplegen via de website. Op de website wordt enkele informatie gegeven over de privacy van bezoekers. Er wordt niet specifiek gewezen op personen die daadwerkelijk een klacht indienen.[35]

[32] Zie bijlage II voor Privacybeleid 2017, gedragscode laatste pagina.
[33] Zie bijlage II voor Privacybeleid 2017, gedragscode laatste pagina.
[34] www.radar.nl.
[35] Zie bijlage III voor figuur 1, Informatieverstrekking (website RADAR).

3. Werkwijze van RADAR

In dit hoofdstuk wordt de werkwijze in de praktijk geschetst. Er zal beschreven worden op welke wijze klachten kunnen worden ingediend. Vervolgens wordt er beschreven welke categorieën persoonsgegevens worden verzameld. Verder wordt er ingegaan op de bijzondere persoonsgegevens. Daarnaast wordt de wijze van de verwerking uiteengezet. Het huidige- en toekomstige registratiesysteem worden beschreven en de beveiliging van de systemen en papieren dossiers worden uiteengezet. Tot slot wordt duidelijk wat de wijze van bewaren en informeren aan derden en cliënten is.

§ 3.1 Protocol klachtbehandeling

Het protocol, dat team klachtbehandeling hanteert voor de verwerking van persoonsgegevens, zal worden toegelicht in de volgende paragrafen. Zoals genoemd in paragraaf 2.3 is het protocol te raadplegen via de website van RADAR. In bijlage I kan het gehele protocol worden geraadpleegd.[36] Na observering en gesprekken blijkt dat in de praktijk niet aan alle stappen wordt toegekomen die het protocol hanteert. In bijlage II kunnen de observatie en gespreksverslagen worden ingezien. In dit hoofdstuk zullen alleen de onderdelen van het protocol worden behandeld die gebruikt worden in de praktijk en waar gegevensverwerking aan te pas komt.

§ 3.2 De wijze van indienen klacht

RADAR maakt onderscheid tussen het indienen van een klacht en het doen van een melding. Indien er een melding wordt gedaan, betekend dit dat er geen verdere onderzoek naar de melding zal plaatsvinden. Een melding wordt enkel geregistreerd in het registratiesysteem voor latere eventuele onderzoeken en statistieken gericht op discriminatie. In paragraaf 3.3 wordt nader toegelicht hoe de verwerking van een melding in het registratiesysteem geschiedt. Indien er een klacht wordt ingediend worden de verschillende stappen doorlopen. Een klacht kan op verschillende wijze worden ingediend bij RADAR. Onderstaand worden de verschillende wijze beschreven.

<u>Klachtformulier:</u>

Middels een klachtformulier dat op de website van RADAR te raadplegen is, kan er een klacht worden ingediend. In dit formulier wordt er gevraagd naar een korte omschrijving van de klacht. De discriminatiegrond moet door betrokkene worden ingevuld. Er wordt hier gebruik gemaakt van een keuzeveld. Er is een aantal discriminatiegronden opgesomd namelijk ras/afkomst, sekse, seksuele gerichtheid, geloofsovertuiging, leeftijd, handicap/chronische ziekte of anders. Achter deze kolom staat een rood sterretje (*) aangegeven. Dit betekent dat dit een verplicht in te vullen veld is. De volgende gegevens die worden gevraagd zijn de naam, adres, postcode, woonplaats, telefoonnummer, e-mailadres, geslacht en etnische afkomst. Tot slot wordt er gevraagd waar de indiener RADAR van kent. De naam, woonplaats en e-mailadres zijn verplicht in te vullen velden. Het formulier moet vervolgens worden verstuurd met een button waarop geklikt moet worden. Vervolgens neemt de klachtbehandelaar zelf contact op met de betrokkene. Uit de gesprekken gedurende de observaties is gebleken dat de klachtbehandelaars individueel kunnen beslissen op welke wijze ze contact opnemen met de betrokkene.[37]

<u>E-mail:</u>

Op de website van RADAR worden er een aantal e-mailadressen weergegeven.[38] Elke locatie, Rotterdam-Rijnmond en Zuid-Holland-Zuid, Midden-en West-Brabant, Brabant-Noord en Zuidoost-Brabant hebben, aparte e-mailadressen. De betrokkene heeft zelf de keuze naar welke regio de e-mail verzonden wordt. Uit het landelijke protocol klachtbehandeling blijkt dat de woonplaats van de betrokkene leidend is.[39] Dit zal dan ook betekenen dat de betrokkene intern wordt doorgezet naar de klachtbehandelaar van de desbetreffende regio. Medewerkers van het bedrijfsbureau hebben het beheer over de e-mailboxen. Zij verdelen de klachten onderling op basis van het dienstrooster.

---

[36] Zie bijlage I voor protocol klachtbehandeling.
[37] Zie bijlage IV voor observatie en gespreksverslag klachtbehandelaar Rotterdam.
[38] 'Contact opnemen', Read, www.radar.nl (zoek op *contact*).
[39] Zie bijlage I voor protocol klachtbehandeling.

Op dit dienstrooster staat welke klachtbehandelaar het betreffende dagdeel dienst heeft. Dienst hebben wil zeggen dat de klachten die dagelijks binnenkomen, per regio, door de aangewezen klachtbehandelaar worden behandeld.[40] Indien er een klacht wordt ingediend via discriminatie.nl dient de melder een postcode in te vullen. De klacht wordt dan automatisch verstuurd naar het RADAR e-mailadres van de regio waar de melder woont. Indien er via discriminatie.nl klachten worden ingediend waarvan de woonplaats Rotterdam is, komen de klachten in de algemene e-mail van RADAR terecht namelijk, info@radar.nl. De klachten worden vervolgens door een medewerker van het bedrijfsbureau, onderverdeeld per regio.[41]

Telefonisch:

Klachten kunnen ook telefonisch worden ingediend. Er staan verschillende telefoonnummers op de website waar RADAR op bereikt kan worden.[42] Uit gesprekken en observaties met de klachtbehandelaars blijkt dat de medewerkers van het bedrijfsbureau de telefoon aannemen. De klachtbehandelaar geeft aan dat het weleens voorkomt dat de cliënt, de klacht al aan de medewerker van het bedrijfsbureau voorlegt. Tijdens het melden van de klacht, noteert de medewerker van het bedrijfsbureau de persoonsgegevens en zet deze in een e-mail naar een klachtbehandelaar. Een klachtbehandelaar neemt in eerste instantie zelf nooit de telefoon op. Indien er een telefonische klacht of melding wordt gedaan, wordt er in ieder geval de persoonlijke gegevens en een korte omschrijving van de klacht opgenomen. Wanneer de klachtbehandelaar op dat moment geen tijd heeft, wordt de cliënt binnen twee werkdagen teruggebeld.[43]

WhatsApp:

Uit gesprekken met de medewerkers team klachtbehandeling blijkt dat er ook klachten kunnen worden ingediend door middel van WhatsApp.[44] Op de website is kenbaar gemaakt dat RADAR vanaf 1 juli 2016 te bereiken is via WhatsApp berichten. Het telefoonnummer is uitsluitend in gebruik voor WhatsApp berichten en niet voor telefonisch contact. Telefonische meldingen kunnen gedaan worden volgens bovenstaande beschrijving.[45] De WhatsApp telefoon wordt door één klachtbehandelaar beheerd. Bij deze klachten worden veelal geen persoonsgegevens uitgewisseld. De ervaring in de praktijk leert dat cliënten veelal anoniem een melding willen indienen.[46]

Persoonlijk:

Eenieder kan op werkdagen tussen 09:00 en 17:00 een klacht indienen. Op alle locaties is momenteel de mogelijkheid om binnen te lopen zonder afspraak. Uit de observaties en gesprekken blijkt dat in de praktijk zelden iemand op kantoor binnenloopt.[47]

In alle bovenstaande gevallen neemt de klachtbehandelaar contact op met de cliënt. Er is niet vastgelegd op welke wijze dit dient te gebeuren. Uit gesprekken met de klachtbehandelaars blijkt dan ook dat de klachtbehandelaar zelf mag overwegen van welke wijze er gebruikt wordt gemaakt. Indien cliënt aangeeft enkel advies te willen, wordt er eerder besloten om een e-mail terug te sturen. Mocht er uit de klacht van cliënt blijken dat deze een luisterend oor nodig heeft, dan kiest de klachtbehandelaar ervoor om cliënt te bellen.[48] In de volgende paragraaf wordt er uiteengezet welke categorieën persoonsgegevens worden verwerkt na het indienen van de klacht volgens bovenstaande wijze.

---

[40] Zie bijlage V voor observatie en gespreksverslag Brabant.
[41] Zie bijlage VI voor mailcorrespondentie bedrijfsbureau.
[42] Contact opnemen, RADAR, www.radar.nl (zoek op *contact*).
[43] Zie bijlage V voor observatie en gespreksverslag Brabant.
[44] Zie bijlage V voor observatie en gespreksverslag Brabant.
[45] 'RADAR nu ook via WhatsApp', Read, www.radar.nl (zoek op *RADAR nu ook via WhatsApp*).
[46] Zie bijlage V voor observatie en gespreksverslag Brabant.
[47] Zie bijlage VII voor observatie en gespreksverslag Rotterdam-Brabant.
[48] Zie bijlage IV voor observatie en gespreksverslag Rotterdam.

§ 3.3 De categorieën persoonsgegevens

Om de klacht te registeren, verzamelt de klachtbehandelaar een aantal persoonsgegevens. In de onderstaand tabel 1: registratie persoonsgegevens, wordt genoemd welke persoonsgegevens, bijzondere persoonsgegevens en welke discriminatiegronden worden verwerkt.

Algemene persoonsgegevens	Bijzondere persoonsgegevens (verplicht in te vullen *)	Keuze discriminatiegronden (optioneel, op grond van klacht)
Naam, achternaam en woonplaats	Nationaliteit	Arbeidscontract
Adres	Herkomst *	Arbeidsduur
Geslacht		Burgerlijke staat
E-mailadres		Geslacht
Telefoonnummer		Godsdienst
Geboortedatum		Handicap
		Leeftijd
		Levensovertuiging
		Nationaliteit
		Niet-wettelijke gronden
		Politieke gezindheid
		Ras
		Seksuele geaardheid

Tabel 1: Registratie persoonsgegevens

Naast de gegevens van de melder worden ook de gegevens van de wederpartij ingevuld. In de praktijk blijkt dat het een keuze is om deze velden in te vullen. De klachtbehandelaar in Rotterdam vult vrijwel nooit de gegevens in van de tegenpartij, in het veld wat daarvoor bedoeld is. Zij vult op een andere pagina, de persoonsgegevens van de tegenpartij in.[49] De klachtbehandelaar die in alle regio's werkt, vult de gegevens van de wederpartij in, op het moment dat het dossier wordt gesloten.[50] De klachtbehandelaar, werkzaam in Brabant, vult altijd de gegevens in van de wederpartij.[51] Uit tabel 1 blijkt dat een aantal persoonsgegevens verplicht zijn in te vullen. In de volgende paragraaf staat beschreven hoe de klachtbehandelaars in de praktijk hiermee omgaan.

§ 3.3.1 De bijzondere persoonsgegevens

RADAR verwerkt ook bijzondere persoonsgegevens. Bij het registeren van de in tabel 1 genoemde bijzondere persoonsgegevens blijkt dat in de praktijk niet op dezelfde wijze geregistreerd wordt. Zo blijkt dat de klachtbehandelaars van Rotterdam-Brabant en Brabant altijd de herkomst van de cliënt invullen. De andere klachtbehandelaar van Rotterdam vult alleen de herkomst in als de klacht discriminatiegrond 'ras' betreft.[52] In het registratiesysteem staat een rode ster (*) achter herkomst. Dit duidt op een verplicht in te vullen veld. Indien er een klacht wordt ingediend op grond van handicap, ras, godsdienst, stafrechtelijk verleden of seksuele leven, dan worden dit bijzondere persoonsgegevens genoemd. Ook een lidmaatschap van een vakvereniging en het Burgerservicenummer (BSN) zijn bijzondere persoonsgegevens. Team klachtbehandeling verwerkt nooit een BSN. Vrijwel alle gronden waarop klachten worden ingediend, vallen onder bijzondere persoonsgegevens. In paragraaf 3.4 wordt er uiteengezet op welke manier de persoonsgegevens verwerkt worden.

[49] Zie bijlage IV voor observatie en gespreksverslag Rotterdam.
[50] Zie bijlage VII voor observatie en gespreksverslag Rotterdam-Brabant.
[51] Zie bijlage IV voor observatie en gespreksverslag Brabant.
[52] Zie bijlage VIII voor conclusies observaties en gespreksverslagen.

§ 3.4 De wijze van verwerking

§ 3.4.1 Het registratiesysteem LBA-net

Alle digitale verwerkingen van RADAR komen terecht in het registratiesysteem genaamd 'LBA-net'. Van dit registratiesysteem maken vrijwel alle antidiscriminatiebureaus (ADB'S) gebruik. LBA-net is een afkorting voor Landelijke Brancheorganisaties van Antidiscriminatiebureaus.[53] De installatie en onderhoud van dit registratiesysteem heeft RADAR uitbesteed aan een externe partij genaamd Constant-IT. Constant-IT verzorgt het beheer en de ondersteuning van de werkstations en servers.[54] Het onderhoud van registratiesysteem binnen RADAR wordt onder andere aangestuurd door een intern contactpersoon van team onderzoek. De contactpersoon van RADAR correspondeert met het extern ICT-bedrijf (Constant-IT) die verantwoordelijk is voor het maken en onderhouden van het registratiesysteem.

§ 3.4.2 Registratiewijze (intern)

De klachtbehandelaars hebben verschillende werkwijzen bedacht om een overzicht te houden van welke en hoeveel klachten er binnenkomen. Er zijn hiervoor registratielijsten per regio opgesteld. Alvorens een klacht wordt verwerkt in het registratiesysteem, wordt deze genoteerd in de registratielijst. In de praktijk blijkt dat dit op twee verschillende manieren wordt gedaan. Rotterdam-Rijnmond en Zuid-Holland-Zuid maken gebruik van een fysieke registratielijst/boek. In dit boek wordt elke klacht van het huidige kalenderjaar die binnenkomt genoteerd. De volgende gegevens worden opgeschreven door de klachtbehandelaars: het LBA-nummer, een eigen logboeknummer, de aantallen, de naam van de melder, datum indienen klacht, klachtbehandelaar en de afsluitdatum.[55] De regio's Midden- en West-Brabant en Brabant-Noord maken gebruik van een digitale registratielijst. Dit is een word-document dat op de gezamenlijke SharePoint wordt opgeslagen. Elke klachtbehandelaar dient deze lijst individueel aan te vullen. In deze registratielijst worden de volgende gegevens genoteerd: de aanmelddatum, de naam van de cliënt, de gemeente van de melder en plaats incident, een omschrijving van de klacht, welke klachtbehandelaar de klacht behandelt en de vervolgstappen (wat te doen).[56]

§ 3.4.3 De wijze van verwerking in het registratiesysteem

Na het aanhoren van de klacht door de klachtbehandelaar wordt er overgegaan op registratie. Het registratiesysteem geeft verschillende mogelijkheden om persoonsgegevens in te vullen. Enkele velden zijn vrij in te vullen. Er kan hier door de klachtbehandelaar zelf een tekst worden getypt. Daarnaast zijn er ook keuzevelden. Dit worden dropdownmenu 's genoemd.[57] De discriminatiegronden worden ingevuld op basis van een keuzeveld. Er staat een aantal gronden aangegeven in LBA-net waar de klachtbehandelaar een verplichte keuze uit moet maken. Er staat namelijk een rode ster (*) achter de discriminatiegrond. De klachtbehandelaar kan kiezen uit de volgende gronden: arbeidscontract, arbeidsduur, burgerlijke staat, geslacht, godsdienst, handicap, leeftijd, levensovertuiging, nationaliteit, niet-wettelijke gronden, politieke gezindheid, ras en seksuele gerichtheid. Indien er wordt gekozen voor bijvoorbeeld een discriminatie gericht op godsdienst, wordt er vervolgens door een keuzeveld aangeboden om aan te geven welke godsdienst de klacht betreft. Vervolgens is het verplicht om in te vullen wat de aard van de klacht betreft. Dit wordt wederom ingevuld door middel van een keuzeveld. De opties bij aard van de klacht zijn vijandige bejegening, omstreden behandeling, bedreiging, mishandeling, gewelddadige groepsconfrontatie, vernieling, brandstichting, doelbekladding, overige gewelddadige uitingen en overig.

---

[53] Coenders, M., J. Kik, E. Schaap, J. Silversmith en R. Schriemer (2012). Kerncijfers 2011. Overzicht van discriminatieklachten en –meldingen geregistreerd bij antidiscriminatievoorzieningen. Leeuwarden / Nijmegen: Landelijke Brancheorganisatie van Antidiscriminatiebureaus (LBA) en Samenwerkende Antidiscriminatievoorzieningen Nederland (SAN).

[54] 'Meldpunt discriminatie regio Amsterdam', referenties, www.constant-it.nl (zoek op *meldpunt discriminatie regio Amsterdam*).

[55] Zie bijlage IV voor observatie- gespreksverslag Rotterdam.

[56] Zie bijlage VII voor observatie en gespreksverslag Rotterdam-Brabant.

[57] Zie bijlage IX voor offerte Constant-IT, blz. 2.

Na het invoeren van de dossiers krijgen deze een status. Dossiers kunnen de volgende statussen hebben: open/gesloten/hoor/wederhoor of alleen registratie.[58]

§ 3.4.4 Beveiliging en toegang digitale gegevens en papieren dossiers

Alle digitale gegevens worden opgeslagen in het registratiesysteem. De beveiliging omtrent de digitale persoonsgegevens is geregeld door Constant-IT. In de offerte van Constant-IT is opgenomen dat ze gebruik maken van SSL-certificaten (encryptie) om de beveiliging te waarborgen. Constant-IT maakt dagelijks een back-up op de Hosting server. Om te zorgen dat dossiers niet verloren gaan, maakt Constant-IT een off-site back-up.[59]
In de offerte is opgenomen dat individuele bureaus uitsluitend toegang hebben tot eigen dossiers. Klachtbehandelaars moeten alleen klachten kunnen administreren uit eigen regio.[60] In de praktijk blijkt dat alle klachtbehandelaars in elke regio kunnen inloggen. Een klachtbehandelaar geeft aan dat een reden hiervan is dat zaken eenvoudig kunnen worden overgenomen als er sprake is van ziekte.[61] Gedurende de observaties en gesprekken en uit ervaring in het werkveld is er geconstateerd dat medewerkers de computer niet vergrendelen bij het verlaten van de werkplek. Daarnaast is geconstateerd dat één locatie van RADAR nog gebruik maakt van papieren dossiers. Indien er stukken zijn opgestuurd, aangeleverd of simpelweg worden geprint, worden deze bewaard in kluizen. Het blijkt dat de papieren dossiers vrijwel de gehele dag kunnen worden ingezien of meegenomen. De kluis waar het lopende archief zich in bevind, staat op een kamer bij een drietal medewerkers. Het andere archief zit in een kluis, staat op een andere kamer en is afgesloten met een sleutel waar één medewerker van het bedrijfsbureau de beschikking over heeft.[62]

Het ICT-bedrijf Trends beheert zaken rondom de beveiliging van het algemene computersysteem en de e-mail (outlook). Er zijn geen duidelijke afspraken of protocollen gericht op de beveiliging van gegevens en outlook opgesteld voor RADAR door Trends. RADAR heeft in opdracht van Trends een KMC Security scan laten uitvoeren om de status van de beveiliging van het bedrijfsnetwerk te laten testen. De uitslagen hiervan zijn toegevoegd in de bijlage. De computers van RADAR hebben alleen toegang met servers en data via een internetverbinding. De internetverbinding van Trends loopt via een VPN-tunnel. Daarnaast zijn computers voorzien van antivirussoftware. Wachtwoorden moeten om de 90 dagen vernieuwd worden op basis van complexiteit. Trends maakt gebruik van digitale certificaten voor Office 365 en Windows DC. Er wordt geen gebruik gemaakt van eigen certificaten, maar vertrouwde certificaten. Office 365 heeft geen Fronted scanning, maar herkent wel verdachte code. Daarnaast is er een lokale virusscanner, alleen bij thuisgebruik is dit niet bekend of wordt niet afgedwongen.[63]

§ 3.4.4.1 Toekomstig registratiesysteem

Vanaf januari 2018 zal het nieuwe registratiesysteem ‘ADV-net’ worden gelanceerd voor RADAR. ADV staat voor antidiscriminatievoorzieningen. Dit registratiesysteem wordt ontwikkeld en beheerd door een extern ICT-bedrijf namelijk ‘Enigmatry’. Uit een interview met een contactpersoon van RADAR team onderzoek, is gebleken dat er voor een nieuw registratiesysteem is gekozen omdat de beveiliging van het oude systeem niet meer voldoet. Het nieuwe registratiesysteem ‘ADV-net’ gaat gebruikmaken van SSL-veiligheidscertificaten ter beveiliging. Ze gaan gebruikmaken van Betty Blocks. Betty Blocks is een systeem voor apps die gebouwd kunnen worden zonder te programmeren. Betty Blocks geeft het volgende aan: *"Betty Blocks beschouwt beveiliging niet als optioneel, dus daarom hebben we onze visie op veiligheid afgestemd op de drie pijlers van informatiebeveiliging, beter bekend als CIA, die staat voor Vertrouwelijkheid, Integriteit & Beschikbaarheid."*[64]

---

[58] Zie bijlage IX voor offerte Constant-IT, blz. 2.
[59] Zie bijlage IX voor offerte Constant-IT, blz. 3.
[60] Zie bijlage IX voor offerte Constant-IT, blz. 2.
[61] Zie bijlage IV voor observatie en gespreksverslag Rotterdam.
[62] Zie bijlage VII voor observatie en gespreksverslag Rotterdam-Brabant.
[63] Zie bijlage IX voor offerte Constant-IT, laatste pagina.
[64] ‘ISO Certified’, www.bettyblocks.com (zoek op *ISO Certified*).

In bijlage X is na het interview, een document toegevoegd met wat ‘OWASP’ inhoudt. OWASP is een lijst met veiligheidsmaatregelen waar tenminste aan gedacht moet worden bij het ontwikkelen en vervolgens beheren van webapplicaties. Er wordt bijvoorbeeld gewaarschuwd om altijd alle input te controleren. Dit omdat anders de webapplicatie gevoelig kan zijn voor een cross side scripting aanval. OWASP gaat verder en adviseert ook om aan andere zaken te denken zoals het systeem waarop je webapplicatie draait (security misconfiguration). Een voorbeeld van security misconfiguration is dat je een applicatie server installeert en het default account niet aanpast, waardoor vrijwel de hele wereld kan inloggen op jouw applicatie server omdat dit account in de installation guide met username en password genoemd is en vindbaar is voor iedereen.[65] De OWASP Top 10 is een overzicht van typen kwetsbaarheden die onder beveiligingsexperts worden gezien als het meest kritisch met betrekking tot webapplicaties. Het is geen kant-en-klare afvinklijst en dekt bovendien niet álle soorten kwetsbaarheden, maar biedt wel een goed zicht op deze complexe materie. De top 10 vormt daarmee een solide basis voor de aangeboden beveiligingstests.[66] De geïnterviewde contactpersoon geeft aan dat in het oude systeem de herkomst en nationaliteit van melder en slachtoffer geregistreerd kon worden. In het nieuwe systeem bestaat deze mogelijkheid nog steeds, maar wordt nu onder een extra knop geplaatst. De gedachte hierachter is dat klachtbehandelaars die met het systeem werken minder geneigd zullen zijn om de herkomst bijvoorbeeld altijd automatisch in te vullen.[67]

§ 3.4.4.2 Meldplicht datalekken

Uit een interviewgesprek met een medewerker van team onderzoek is gebleken dat er geen protocol bestaat voor hoe te handelen bij een datalek. Verder geeft deze medewerkster aan dat ze niet weet of er ooit een datalek heeft plaatsgevonden.[68] Uit observaties en gesprekken is gebleken dat klachtbehandelaars ook niet weten of dit in de praktijk ooit heeft plaatsgevonden.[69]

§ 3.5 De behandeling van een klacht

Na het registeren van de klachten kan de klachtbehandelaar ervoor kiezen om een intakegesprek te voeren. De cliënt ontvangt informatie over de dienstverlening en wijze van klachtbehandeling van RADAR. Tevens wordt de cliënt gevraagd om relevante documenten mee te nemen. Geeft het slachtoffer te kennen door te willen gaan met de zaak, dan wordt het principe van hoor en wederhoor toegepast. Dit betekent dat de wederpartij om diens visie op het gebeurde wordt gevraagd, voordat wordt besloten om over te gaan tot eventuele actie.[70] In het klachtenprotocol wordt bij het voeren van het intakegesprek een passage opgenomen over registratie en privacybescherming. De cliënt zal geïnformeerd worden over de wijze van dossiervorming en hoe met deze gegevens wordt omgegaan. De persoonsgegevens blijven vertrouwelijk. De cliënt zal worden verteld dat deze persoonsgegevens nooit zonder zijn of haar persoonlijke toestemming beschikbaar worden gesteld aan derden. De cliënt heeft na afspraak recht op inzage in het dossier. In de praktijk blijkt dat er niet altijd een intakegesprek plaatsvindt. Om deze reden wordt de informatie over privacy niet structureel door klachtbehandelaars medegedeeld aan cliënten.[71] Na beëindiging van het intakegesprek wordt een verslag opgesteld en aangevuld met een advies over de verdere wijze van behandeling. Na het intakegesprek wordt een vooronderzoek ingesteld. Het vooronderzoek richt zich primair op het verkrijgen van aanvullend feitenmateriaal, verklaringen van getuigen en mogelijkheden van aanpak en procedures.[72] De klachtbehandelaar kiest met instemming van de cliënt de te nemen vervolgstappen.

---

[65] ‘Een waakhond voor webapplicaties’, tips en tricks, www. pc-en-internet.infonu.nl (zoek op *Een waakhond voor webapplicaties*).
[66] ‘OWASP Top-10’, www.whitehats.nl (zoek op *OWASP Top-10*).
[67] Zie bijlage X voor interview RADAR team onderzoek.
[68] Zie bijlage X interview RADAR team onderzoek.
[69] Zie bijlage VIII voor conclusie observaties en gesprekken.
[70] Zie bijlage I voor protocol klachtbehandeling, blz. 4-5.
[71] Zie bijlage VIII voor conclusie observaties en gesprekken.
[72] Zie bijlage I voor protocol klachtbehandeling, blz. 7.

Enkele opties die gekozen kunnen worden zijn: hoor-wederhoor, bemiddeling, advies voor eigen handelen, procedure bij de Commissie Gelijke Behandeling of een gerechtelijke procedure. De klachtbehandelaar dient de gekozen strategie te evalueren en de klacht af te sluiten.[73]

§ 3.6 De wijze van informeren aan derden

In hoofdstuk twee is vanuit het eigen privacybeleid duidelijk geworden dat cliënten geïnformeerd moeten worden over hoe er wordt omgegaan met de persoonsgegevens die ze gedeeld hebben. In veel gevallen wordt er na het melden van de klacht gekozen voor bemiddelen. Tijdens het bemiddelen worden er persoonsgegevens van de melder gedeeld met de derde. Naar aanleiding van de verschillende observaties en gesprekken is het onduidelijk op welke manier de toestemming wordt verkregen. Er wordt geen gebruik gemaakt van een toestemmingsformulier. Enkele klachtbehandelaars geven aan dat ze mondeling en/of telefonisch toestemming krijgen om persoonsgegevens met derden te delen.[74]

§ 3.7 De wijze van informeren aan de cliënt

Betrokkene die een klacht indienen bij RADAR hebben altijd recht op inzage in eigen dossier. In de praktijk blijkt dat dit recht niet door alle klachtbehandelaars duidelijk wordt gemaakt aan de cliënt. Uit observaties en gesprekken blijkt dat enkele klachtbehandelaars dit in sommige gevallen mededelen aan betrokkenen. Indien er bijvoorbeeld sprake is van een bemiddelingsgesprek tussen twee partijen, dan deelt de klachtbehandelaar mondeling mee dat het dossier kan worden ingezien.[75] Verder blijkt uit de observaties en gesprekken dat klachtbehandelaars de overige rechten van cliënten niet benadrukken.[76]

§ 3.8 De wijze van bewaren

RADAR team klachtbehandeling maakt in de praktijk gebruik van twee soorten archieven. Er bestaat een lopend archief en een algemeen archief. In het lopend archief zitten papieren dossiers die tot op heden nog gebruikt worden. Dit zijn digitale dossiers die door de medewerker klachtbehandelaar geprint zijn of originele stukken die zijn aangeleverd door cliënten. Uit observaties en gesprekken is gebleken dat klachtbehandelaars op de locatie Rotterdam het lastig vinden om van het lopende archief af te stappen. Ze geven aan dat er open zaken en originele stukken in worden bewaard. Er worden dossiers van het lopende jaar in een map bewaard en oudere dossiers worden in hangmappen bewaard. Daarnaast bestaat er ook een archief waar alleen alle oude papieren dossiers in worden bewaard.[77] De locaties Tilburg en ’s-Hertogenbosch gebruiken geen lopend archief meer. Er bestaat nog wel een algemeen archief waar gesloten dossiers in bewaard worden.[78]

§ 3.8.1 Bewaartermijn

RADAR hanteert voor het bewaren van persoonsgegevens, de bewaartermijn genoemd in de Archiefwet. RADAR heeft gekozen om de papieren dossiers te bewaren voor een periode van vijf jaar. In de offerte van Constant-IT is opgenomen dat digitale dossiers een bewaarduur van een periode van maximaal vijf jaar heeft.[79] In de praktijk blijkt dat voor de digitale dossiers die worden bewaard in het registratiesysteem geen bewaartermijn gehanteerd wordt. Alle dossiers van meer dan vijf jaar geleden zijn zichtbaar voor iedereen en blijken niet geanonimiseerd te zijn.[80]

[73] Zie bijlage I voor protocol klachtbehandeling, blz. 11.
[74] Zie bijlage VIII voor conclusie observaties en gesprekken.
[75] Zie bijlage IV voor observatie en gespreksverslag Rotterdam.
[76] Zie bijlage VIII voor conclusie observaties en gesprekken.
[77] Zie bijlage VII voor observatie en gespreksverslag Rotterdam-Brabant.
[78] Zie bijlage VIII voor conclusie observaties en gesprekken.
[79] Zie bijlage IX voor offerte Constant-IT, blz. 2.
[80] Zie bijlage IV voor observatie en gespreksverslag Rotterdam.

4. Relevante wet- en regelgeving

In dit hoofdstuk staat het huidige juridische kader omtrent de verwerking van persoonsgegevens centraal. Allereerst wordt de aanleiding voor de AVG uiteengezet. Vervolgens wordt er ingegaan op de relevante bepalingen die door RADAR in acht moeten worden genomen.

§ 4.1 De aanleiding van de AVG

Alvorens de AVG werd geïntroduceerd was de Wbp van toepassing.
De Wbp is in de Nederlandse wet geïmplementeerd ter toepassing van de internationale richtlijn 95/46. Ook in de Grondwet zijn een aantal artikelen te vinden ter bescherming van het recht van eerbiediging van de persoonlijke levenssfeer. Dit recht is ook in art. 8 van het EVRM opgenomen. Artikel 8 EVRM heeft een directe werking zodat daarop rechtstreeks een beroep kan worden gedaan.[81] In art. 10 lid 2 van de Grondwet, (hierna: GW), is bepaald dat de wetgever regels dient op te stellen inzake de verwerking van persoonsgegevens.[82] De wetgever heeft hieraan uitvoering gegeven door middel van de Wet persoonsregistraties, die in 1988 in werking trad. Kort hierna werd een wetsvoorstel ingediend om de Wbp in werking te laten treden, waarmee het kader uitgebreider werd.[83] In de praktijk bleek dat er ernstige knelpunten gesignaleerd werden met betrekking tot de uitvoering en de handhaving van de wet. Deze knelpunten hangen nauw samen met de problemen die in de Europese wetgeving zijn geconstateerd. In de praktijk blijkt dat EU-lidstaten aanzienlijke verschillen hebben met de wijze waarop de richtlijn 95/46 in nationale wetgeving is omgezet.[84] Met name om deze reden is de AVG geïntroduceerd.[85] De Wbp zal per 25 mei 2018 volledig worden ingetrokken. De Uitvoeringswet Algemene Verordening Gegevensbescherming (hierna: Uitvoeringswet) bepaalt dat wanneer artikelen uit de Wbp zijn overgenomen, dit in artikelsgewijze toelichting wordt vermeld.[86]

De AVG daarentegen is een direct doorwerkende verordening die in elke aangesloten lidstaat van toepassing zal worden. In de EU heeft nu nog elke lidstaat een eigen privacywet. De verordening heeft als doel dat het niveau van de bescherming van de persoonsgegevens verhoogd wordt. Dit wordt gerealiseerd door in alle lidstaten van de EU, het niveau van de bescherming gelijk te stellen. Deze gelijkheid ontstaat doordat de AVG een verordening is en deze dus niet hoeft te worden omgezet in nationale wetgeving. Bij de Wbp moest dit nog wel. De Wbp komt namelijk voort uit de Privacyrichtlijn 96/46/EG van 24 oktober 1995.[87] Op 4 mei 2016 is de AVG gepubliceerd in het Publicatieblad van de Europese Unie. Er is een periode van twee jaar aangehouden als overgangsperiode. Deze tijd is geboden om de organisaties en toezichthouders in de gelegenheid te stellen zich goed voor te bereiden op de AVG. Per mei 2018 zal de AVG van kracht zijn. De AVG gaat er onder meer voor zorgen dat er versterking en verbreding van de privacyrechten wordt gerealiseerd. De AVG heeft als doel het reguleren van de verwerking van persoonsgegevens. Door deze regulering ontstaat er een markt voor persoonsgegevens. Dit sluit overigens aan op het vrij verkeer van diensten. Vrij verkeer van diensten is een grondrecht binnen de Europese Unie.[88] Als gevolg hiervan zullen er meer verantwoordelijkheden worden neergelegd bij de organisaties.[89]

---

[81] Leidraad, *Afstemmen op de Wet bescherming persoonsgegevens, p.23.*
[82] Kranenborg en Verhey 2011, p. 55.
[83] Kranenborg en Verhey 2011, p. 56.
[84] Richtlijn 95/46/EG (PbEG 1995, L 281/31)
[85] Kranenborg en Verhey 2011, p. 171.
[86] MvT Uitvoeringswet AVG, p. 92.
[87] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 307.
[88] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 13.
[89] 'Algemene informatie AVG, Onderwerpen, AVG nieuwe Europese privacywetgeving, www.autoriteitpersoonsgegevens.nl/ (zoek op *Algemene informatie AVG*).

De AVG is van toepassing op de gehele of gedeeltelijke geautomatiseerde verwerking, en op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen. De relevante bepalingen uit de AVG, die met name voor RADAR van belang zijn, worden in dit hoofdstuk beschreven.

§ 4.1.1 Toepasselijkheid AVG

De AVG is van toepassing op het geheel of gedeeltelijk geautomatiseerde verwerken van persoonsgegevens. De AVG is tevens van toepassing op de non-geautomatiseerde (papier) verwerkingen van persoonsgegevens, die in een bestand zijn opgenomen of bestemd zijn daarin opgenomen te worden. [90] Dit is neergelegd in art. 2 lid 1 van de AVG.[91] Er is sprake van een geautomatiseerde verwerking indien gebruik wordt gemaakt van middelen en methoden van geautomatiseerde verwerking. Iedere handeling via ICT-middelen of internet is al aan te merken als een geheel of gedeeltelijke geautomatiseerde verwerking. [92] Als er bij een onderdeel gebruik wordt gemaakt van handmatige verwerking dan is dit gedeeltelijk geautomatiseerd. De AVG is ook van toepassing op handmatige verwerking van persoonsgegevens als deze in een bestand zijn of worden opgenomen.[93]

§ 4.2 De materiele normen voor gegevensverwerking

§ 4.2.1 Begrippen AVG

Alvorens er wordt ingegaan op de inhoud van de AVG, wordt in de begrippenlijst (te vinden aan het begin van dit rapport) een aantal begrippen opgesomd. In art. 4 van de AVG staan de definities van de begrippen opgesomd. Er worden enkel een aantal begrippen uitgelicht die met name van belang zijn voor dit onderzoek.

§ 4.2.2 Beginselen voor de verwerking

In art. 5 AVG staan alle beginselen opgesomd die gelden voor het rechtmatig verwerken van persoonsgegevens. Een duidelijk verschil is dat in de Wbp de beginselen in meerdere verschillende artikelen zijn beschreven, terwijl in de AVG alle beginselen die in acht genomen moeten worden voor de verwerking van persoonsgegevens in één artikel zijn opgenomen. De beginselen en de betekenis daarvan blijven onveranderd. De verwerkingsverantwoordelijke dient zicht te houden aan de volgende beginselen:

<u>Beginselen van rechtmatigheid, behoorlijkheid en transparantie;</u>

Dit beginsel legt de verwerkingsverantwoordelijke de plicht op om de gegevens rechtmatig, behoorlijk en transparant te verwerken. Met rechtmatig wordt gedoeld op de rechtmatigheid en aanwezigheid van een gerechtvaardigde grondslag. Met behoorlijk en transparant wordt bedoeld dat er op een vertrouwelijke manier met de gegevens wordt omgegaan. De transparantie ziet er op dat het voor de betrokkene duidelijk moet zijn welke gegevens van hem worden verwerkt en met welke reden.[94]

<u>Beginsel van doelbinding;</u>

De verwerkingsverantwoordelijke dient aan te geven waarvoor hij persoonsgegevens verzamelt. De doeleinden dienen gerechtvaardigd te zijn. Er mogen geen gegevens worden verwerkt die niet noodzakelijk zijn om het doel te bereiken. De verwerkingsverantwoordelijke dient zelf te beoordelen of het hergebruik van persoonsgegevens voor andere doeleinden, al dan niet verenigbaar is. Er zal rekening moeten worden gehouden met of er eventueel een verband bestaat tussen de doeleinden waarvoor de gegevens werden verkregen en de doeleinden van de voorgenomen verdere verwerking.

---

[90] 'Wat zijn persoonsgegevens', Over Privacy, Persoonsgegevens, www.autoriteitpersoonsgegevens.nl/ (zoek op *wat zijn persoonsgegevens*).
[91] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 15.
[92] HvJ EU 6 november 2003, zaaknr. C-101/01,Lindqvist.
[93] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 15.
[94] J. Berkvens & C. Jakimowicz, Tekstuitgave Privacyverordening met geïntegreerde overwegingen, Wbp- en Richtlijn 95/46/EG-teksten en verwijstabellen, Den Haag: Boom juridisch 2016, p. 29.

Er dient te worden gekeken naar de context waarin de persoonsgegevens werden verkregen, in het bijzonder gelet op de relatie tussen betrokkenen en de verantwoordelijke voor de verwerking. Met de aard van de persoonsgegevens met name verwerking die slaat op bijzondere categorieën persoonsgegevens moet rekening worden gehouden en met de mogelijke gevolgen van de voorgenomen, verdere verwerking voor betrokkenen. Tot slot moet er gekeken worden naar het bestaan van de passende waarborgen, waaronder eventueel versleuteling of pseudonimisering. Wanneer de betrokkene zijn toestemming heeft gegeven, mag de verwerkingsverantwoordelijke de persoonsgegevens verder verwerken, ongeacht of dat verenigbaar is met de doeleinden.[95]

Beginsel van minimale gegevensverwerking;

De persoonsgegevens moeten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. De verwerkingsverantwoordelijke moet rekening houden met het principe van 'minimale gegevensverwerking'. Het beginsel van dataminimalisatie brengt met zich mee dat niet meer persoonsgegevens verwerkt mogen worden dan strikt noodzakelijk is voor het doel.[96] Dit houdt in dat slechts de persoonsgegevens verzameld mogen worden die nodig zijn om de taakvervulling goed te kunnen uitvoeren. De gegevens dienen toereikend, ter zake dienend en beperkt te zijn tot wat noodzakelijk is voor de verwerker om de doeleinden van deze verzameling te bereiken. Het uitgangspunt is dus dataminimalisatie.[97]

Beginsel van juistheid;

De persoonsgegevens dienen juist en actueel te zijn. Blijkt het dat gegevens onjuist of achterhaald zijn, dan moeten zij worden gewist. Dit beginsel is nader uitgewerkt in de rechten van rectificatie genoemd in paragraaf 4.4. De verwerkingsverantwoordelijke dient zelfstandig en actief zorg te dragen voor de juistheid van de persoonsgegevens die hij onder zich heeft.[98]

Beginsel van opslagbeperking;

De persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk is. Er dient gezorgd te worden voor een passende beveiliging voor de persoonsgegevens en de persoonsgegevens moeten juist, actueel, toereikend en ter zake dienend zijn. De AVG noemt geen termijnen voor het bewaren van de persoonsgegevens. Diverse wetgeving verplichten de verwerkingsverantwoordelijke om bepaalde gegevens te bewaren gedurende een bepaalde periode. Dit wordt door de AVG gerechtvaardigd op grond van art. 6 AVG lid 1 sub c. Daaruit volgt dat gegevens bewaard mogen worden gedurende de wettelijke termijn.[99]

Beginsel van integriteit en vertrouwelijkheid;

Om de integriteit en vertrouwelijkheid te waarborgen, dient de verwerkingsverantwoordelijke technische en organisatorische beveiligingsmaatregelen te treffen. Dit om ongeoorloofde toegang en het ongeoorloofde gebruik van persoonsgegevens te voorkomen. Dit beginsel wordt nader uitgewerkt en gekoppeld aan de datalekmeldplicht in paragraaf 4.3.4.[100]

De beginselen van proportionaliteit en subsidiariteit;

Het evenredigheids- of proportionaliteitsbeginsel houdt in dat de inbreuk op de belangen van de betrokkene niet onevenredig mag zijn in verhouding tot het met de verwerking te dienen doel. Het vergt een belangenafweging aan de hand van omstandigheden van het concrete geval.

---

[95] 'Het beginsel van de doelbinding', Privacycommission, www.privacyscommission.be (zoek op *het beginsel van de doelbinding*).

[96] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 41.

[97] 'Rechtmatigheid en Transparantie', algemene verordening gegevensbescherming, europadecentraal.nl (rechtmatigheid en transparantie).

[98] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 41.

[99] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 42

[100] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 42

De grens ligt daar waar het middel niet in verhouding staat tot het doel, want dan is het optreden buiten proportie. Het subsidiariteitsbeginsel wordt beschouwd als een factor die een rol speelt in het kader van de evenredigheidstoets. Het doel waarvoor de persoonsgegevens worden gebruikt, dient in redelijkheid niet op een andere, minder nadelige wijze te kunnen worden verwerkelijkt. Op de verwerkingsverantwoordelijke rust de plicht om binnen redelijke grenzen een inbreuk op de persoonlijke levenssfeer te vermijden dan wel zo beperkt mogelijk te houden.[101]

§ 4.2.3 De rechtmatigheid van de verwerking

De verwerking van persoonsgegevens dient in overeenstemming te zijn met de bovenstaande beginselen voor een rechtmatige verwerking. Uit bovenstaande beginselen blijkt dat verwerking van de persoonsgegevens op een behoorlijke en zorgvuldige wijze dient plaats te vinden. Ook dient de gegevensverwerking noodzakelijk te zijn voor een goede vervulling van de taak. Dit wordt rechtmatigheid genoemd. Persoonsgegevens mogen alleen worden verwerkt voor ‘’welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden’’. Het doel waartoe men de persoonsgegevens verwerkt moet dus uitdrukkelijk zijn weergegeven. Met ‘welbepaalde’ bedoelt de wetgever, dat het doel vast moet staan alvorens men overgaat tot het verzamelen van de persoonsgegevens. Het vereiste dat de verwerking gerechtvaardigd dient te zijn, wordt nader uitgewerkt in art. 6 AVG.[102] In art. 6 AVG wordt een limitatieve opsomming van gerechtvaardigde doeleinden uiteengezet. De persoonsgegevens dienen overeen te stemmen met in ieder geval één van de gerechtvaardigde doelen in art.6 AVG. De persoonsgegevens dienen in overeenstemming met in ieder geval één van de gerechtvaardigde doelen in art.6 AVG overeen te komen.[103] Alle vereisten van art. 6 AVG dienen in overeenstemming te zijn met de beginselen van proportionaliteit en subsidiariteit. De limitatieve lijst met rechtmatigheidsgronden worden navolgend opgesomd:

<u>Verwerking op grond van toestemming (art. 6 lid 1 sub a AVG);</u>
De betrokkene heeft toestemming gegeven om persoonsgegevens te verwerken. Toestemming houdt in dat het een vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting moet zijn. De betrokkene aanvaardt met deze toestemming dat zijn persoonsgegevens verwerkt worden.

<u>Verwerking ter uitvoering van een overeenkomst (art. 6 lid 1 sub b AVG);</u>
Deze rechtmatigheidsgrond geeft de verwerkingsverantwoordelijke de mogelijkheid om persoonsgegevens te verwerken, indien dit noodzakelijk is voor de uitvoering van een overeenkomst. Slechts wanneer de overeenkomst niet kan worden nagekomen zonder verwerking, is gegevensverwerking noodzakelijk.[104]

<u>Verwerking om te voldoen aan een wettelijke verplichting (art. 6 lid 1 sub c AVG);</u>
Indien vanuit de wet wordt bepaald dat instanties persoonsgegevens dienen te verwerken, wordt dit gezien als ‘verwerking om te voldoen aan een wettelijke verplichting’. De instantie dient alleen de persoonsgegevens te verwerken die noodzakelijk zijn om aan de wet te voldoen. Dit wordt het noodzakelijkheidsvereiste genoemd. Hierbij kan worden gedacht aan de verplichting voor banken om jaarlijks gegevens van hun rekeninghouders aan de Belastingdienst te verstrekken ten behoeve van de belastingheffing (artikel 22 van het Uitvoeringsbesluit inkomstenbelasting 2001).[105]

---

[101] Mr. C.W.J.M. Ebbers & dr. Ir. J, van Hoof & ir. C.E. Oude Weernink, *Privacyaspecten van track-en-tracetechnologie in de zorg*, p. 29.
[102] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 43.
[103] ‘Rol van toestemming in het sociaal domein’, Autoriteit Persoonsgegevens, 19 april 2016.
[104] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 44
[105] MvT Uitvoeringswet AVG, p. 29.

Verwerking om de vitale belangen van een natuurlijk persoon te beschermen (art. 6 lid 1 sub d AVG);
Als vierde grondslag is verwerking toegestaan, indien dit noodzakelijk is voor de vitale belangen van de betrokkene of een andere persoon. Een vitaal belang moet zien op het leven van die persoon. Hierbij kan er worden gedacht aan medische noodsituaties. In beginsel is het toekennen van deze grond, alleen toegestaan indien de verwerking niet op een andere rechtsgrond kan worden gebaseerd.[106]
Verwerking ter vervulling van een taak van algemeen belang of uitoefening openbaar gezag (art. 6 lid 1 sub e AVG);
Een verwerking van persoonsgegevens is gerechtvaardigd indien deze noodzakelijk is voor een taak van algemeen belang of taak voor het openbaar gezag. Het algemeen belang beperkt zich in ieder geval niet alleen tot overheidsinstanties.[107]
Verwerking in het belang van de verwerkingsverantwoordelijke (art. 6 lid 1 sub f AVG);
Wanneer verwerking plaatsvindt als dit nodig is voor, het behartigen van een gerechtvaardigd belang van de verwerkingsverantwoordelijke, wordt dit gezien als rechtmatig. Verwerking moet noodzakelijk zijn om aan dit gerechtvaardigde belang te voldoen. Er dient een belangenafweging met de grondrechten van de betrokkene plaats te vinden. Het belang van de verwerkingsverantwoordelijke dient zwaarder te wegen dan de fundamentele vrijheden, de grondrechten en belangen van de betrokkene.[108]

§ 4.2.4 Vereisten voor verwerking van bijzondere persoonsgegevens

Bijzondere persoonsgegevens betreffen naar hun aard zeer gevoelige informatie. Persoonsgegevens die betrekking hebben op ras etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond en verwerking van genetische en biometrische gegevens, kunnen als gevoelig worden aangemerkt. Verwerking van deze gegevens kan een grote inbreuk leveren op de persoonlijke levenssfeer van betrokkene. Indien deze gegevens toch verwerkt worden, zijn daarop strengere eisen van toepassing dan op de verwerking van persoonsgegevens in het algemeen. De bijzondere persoonsgegevens worden opgesomd in art. 9 AVG. Het uitgangspunt van de AVG is dat bijzondere persoonsgegevens niet verwerkt mogen worden, tenzij één van de rechtvaardigingsgronden van toepassing is. De rechtvaardigingsgronden die voor dit onderzoek van belang zijn, worden hieronder uiteengezet:
Verwerking op grond van toestemming (art. 9 lid 2 sub a AVG);
De eerdergenoemde grond voor, de rechtmatige verwerking op grond van toestemming, in art. 6 AVG lid 1 sub a, geldt tevens voor het verwerken van bijzondere persoonsgegevens.
Verwerking is noodzakelijk met het oog op de uitvoering van verplichtingen ten behoeve van het arbeids-, sociaalzekerheids- of socialebeschermingsrecht (art. 9 lid 2 sub b AVG);
Indien het noodzakelijk is om bijzondere persoonsgegevens te verwerken, gericht op wettelijke plichten of rechten binnen de boven genoemde rechtsgebieden, dan is deze verwerking toegestaan voor de verwerkingsverantwoordelijke. Dit dient wel in een wettelijke regeling of dergelijk cao te zijn vastgelegd. [109]
Verwerking is noodzakelijk voor de vitale belangen van een natuurlijk persoon (art. 9 lid 2 sub c AVG);
Verwerking van bijzondere gegevens kan noodzakelijk zijn, als dit ziet op de vitale belangen van een natuurlijk persoon. De betrokkene moet bij deze grond niet in staat zijn om toestemming te geven. In paragraaf 4.2.3 is besproken wat bedoeld wordt met vitale belangen.

---

[106] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 45.
[107] Sauwerwein en Linneman 2002, p. 23.
[108] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 46.
[109] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming.* Artikelgewijs commentaar, Amsterdam: Ius Mentis 2017, p. 59.

Verwerking door bepaalde organisaties zonder winstoogmerk in het kader van gerechtvaardigde activiteiten (art. 9 lid 2 sub d AVG);
Instanties die zonder winstoogmerk opereren zoals politieke partijen, vakbonden of religieuze instellingen mogen persoonsgegevens van haar leden verwerken. Dit geldt alleen voor interne verwerking.[110]
Verwerking van persoonsgegevens die openbaar zijn gemaakt (art. 9 lid 2 sub e AVG);
Gegevens die door de betrokkene openbaar zijn gemaakt, mogen zonder toestemming verwerkt worden. Het gaat hier wel om gegevens die vrijwillig door de betrokkene openbaar zijn gemaakt met het doel deze persoonsgegevens te openbaren. Hierbij kun je denken aan verschillende informatie die op openbare sociale media wordt gedeeld.[111]
Verwerking is noodzakelijk met het oog op archivering in het algemeen belang, wetenschappelijk belang of historisch onderzoek (art. 9 lid 2 sub j AVG);
In de Uitvoeringswet art. 27 is bepaald dat verwerking met het oog op archivering in het algemeen belang, wetenschappelijk belang of historisch onderzoek is toegestaan, indien uitdrukkelijke toestemming vragen onmogelijk of een onevenredige inspanning zou vergen. Wel moeten dan voldoende waarborgen zijn ingesteld zodat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.[112]

De overige rechtvaardigingsgronden worden niet genoemd, omdat zij niet van belang zijn voor dit onderzoek.

4.2.4.1 Toestemming van de betrokkene

In art. 4 lid 11 AVG wordt toestemming gedefinieerd als “elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een duidelijke actieve handeling hem betreffende verwerking van persoonsgegevens aanvaardt”. De toestemming van de betrokkene moet ondubbelzinnig zijn. Dit houdt in dat er voor de verwerkingsverantwoordelijke geen twijfel mag bestaan of de betrokkene bedoelt dat hij akkoord gaat met de verwerking van de persoonsgegevens.[113] De betrokkene dient expliciet zijn wil omtrent de verwerking te hebben geuit. Een stilzwijgende of impliciete toestemming is onvoldoende want ‘de betrokkene dient in woord, schrift of gedrag uitdrukking te hebben gegeven aan zijn wil toestemming te verlenen aan de hem betreffende gegevensverwerking’.[114] Indien er met bijzondere persoonsgegevens wordt gewerkt dient vooraf per definitie uitdrukkelijke toestemming te zijn gegeven. De privacyrisico’s van het verwerken van bijzondere persoonsgegevens zijn groter dan bij normale persoonsgegevens. Daarnaast volgt uit art. 4 lid 11 AVG dat er sprake moet zijn van vrije wilsuiting. Dit betekent dat betrokkene zelf een keuze moet kunnen maken en geen nadelige gevolgen mag ondervinden als hij de toestemming intrekt of weigert.[115] In geval van afhankelijkheidsrelaties met de overheid of een werkgever zou dit zich kunnen voordoen. In de tekst van de wet is ook opgenomen dat de wilsuiting ‘specifiek’ en ‘geïnformeerd’ dient te zijn. Specifiek houdt dit in dat er toestemming moet worden gegeven voor een bepaalde vorm van gegevensverwerking die plaats zal vinden, niet voor gegevensverwerking in het algemeen.[116]

---

[110] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 60.
[111] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 61.
[112] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 64.
[113] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 51.
[114] *Kamerstukken II* 1997/98,25892,3, P. 122.
[115] J. Berkvens & C. Jakimowicz, Tekstuitgave Privacyverordening met geïntegreerde overwegingen, Wbp- en Richtlijn 95/46/EG-teksten en verwijstabellen, Den Haag: Boom juridisch 2016, p. 25.
[116] ‘Wijzigingen Algemene Verordening Gegevensbescherming’, consultancy, www.consultancy.nl (zoek op *Wijzigingen Algemene Verordening Gegevensbescherming*’).

4.2.4.2 Verstrekken van persoonsgegevens aan derde(n)

Het verstrekken van de persoonsgegevens moet op grond van art. 6 AVG verenigbaar zijn met het doel waarvoor de persoonsgegevens verzameld zijn. Bij verenigbaar met het doel spelen verschillende factoren een rol. Er wordt gekeken naar de verwantschap met het doel van verzamelen. De aard van de gegevens. De gevolgen van de verstrekking. De waarborgen die zijn getroffen en de verwachtingen van de betrokkene (cliënt). Persoonsgegevens mogen niet verder verwerkt worden dan de doeleinden die voor de gegevensverwerking gesteld zijn.[117] Gerechtvaardigde doeleinden vloeien voort uit art. 6 AVG. Ondanks deze gerechtvaardigde doeleinden mogen de betreffende gegevens ook voor andere doeleinden worden gebruikt. Dit is overigens alleen toegestaan mits de doeleinden voor de verdere verwerking verenigbaar zijn met het oorspronkelijke doel. Wanneer de oorspronkelijke verwerking heeft plaatsgevonden met toestemming als wettelijke grondslag, dan mag de verwerkingsverantwoordelijke verdere verwerking verrichten zonder het in acht nemen van het onverenigbaar gebruik. Hier wordt door overweging 50 AVG aan toegevoegd dat de beginselen voor een rechtmatige verwerking moeten worden toegepast. Dit houdt in dat de betrokken geïnformeerd dient te worden over het doel van de verdere verwerking en dat de rechten van cliënten ook nadrukkelijk medegedeeld dienen te worden.[118]

§ 4.3 Verplichtingen verwerkingsverantwoordelijke

Voor bedrijven en organisaties die als verantwoordelijke worden gekwalificeerd in de zin van de AVG, zijn er verschillende verplichtingen opgenomen in de AVG. In deze paragraaf zullen de belangrijkste verplichtingen worden beschreven die essentieel zijn voor dit onderzoek. De verwerkingsverantwoordelijke zal onder de AVG veel actiever moeten worden, om ervoor te zorgen dat de verwerking van de persoonsgegevens zo min mogelijk belastend zal zijn voor de betrokkene. Artikel 25 AVG bepaalt dat de verwerkingsverantwoordelijke zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische maatregelen moet treffen, die zijn opgesteld met het doel de gegevensbeschermingsbeginselen op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen ter naleving van de voorschriften van de AVG en ter bescherming van de rechten van de betrokkenen. Om dit te bereiken is er in de praktijk een aantal wijzigingen nodig.

§ 4.3.1 Documentatieplicht

In de AVG wordt meer nadruk gelegd op de verantwoordelijkheid van de organisaties zelf. Er moet door de verwerkingsverantwoordelijke worden aangetoond dat onder andere de verwerkers juiste technische en organisatorische maatregelen hebben genomen om de persoonsgegevens te beschermen. Dit vindt zijn uitwerking in onder andere de documentatieplicht, die is neergelegd in art. 30 AVG. De verwerkingsverantwoordelijke dient een register bij te houden waarin alle verwerkingsactiviteiten staan genoteerd. In dit register dienen de naam en contactgegevens van de verwerkingsverantwoordelijke en van de functionaris voor de gegevensbescherming te worden opgenomen. Verder moeten de verwerkingsdoeleinden en een beschrijving van betrokkenen en persoonsgegevens genoteerd worden. Ook dient er duidelijk te zijn wie de eventuele ontvangers van de persoonsgegevens kunnen zijn. Indien het mogelijk is dient de voorgenomen bewaartermijn en een beschrijving van de technische en organisatorische beveiligingsmaatregelen te worden opgenomen. Voorts blijkt uit dit artikel dat er geen melding meer gedaan hoeft te worden aan de AP wanneer een organisatie voornemens is gegevens (gedeeltelijk) geautomatiseerd te gaan verwerken.

---

[117] Mr. C.W.J.M. Ebbers & dr. Ir. J, van Hoof & ir. C.E. Oude Weernink, *privacyaspecten van track-en-tracetechnologie in de zorg*, p. 27.

[118] J. Berkvens & C. Jakimowicz, Tekstuitgave Privacyverordening met geïntegreerde overwegingen, Wbp- en Richtlijn 95/46/EG-teksten en verwijstabellen, Den Haag: Boom juridisch 2016, p. 231.

De AP vervult een toezichthoudende en controlerende taak. Er wordt steekproefsgewijs bij de organisaties gecontroleerd of zij de documentatieplicht op een juiste manier naleven.[119]

§ 4.3.2 Informatieplicht

De AVG kent er veel gewicht aan toe dat de cliënt geïnformeerd wordt over de verwerkingsdoeleinden van de verzamelde persoonsgegevens. Onder de AVG wordt de informatieplicht dus uitgebreid en moeten er meer gegevens aan de cliënt worden verstrekt op het moment dat de persoonsgegevens worden verzameld. Volgens de AVG moet de informatie eenvoudig toegankelijk en op een begrijpelijke manier zijn afgestemd op de doelgroep. Er moet duidelijke en eenvoudige taal worden gebruikt.[120] Op grond van art. 13 AVG dient er informatie te worden verschaft over wie de verwerkingsverantwoordelijke is. Ook moet er duidelijk zijn of er een FG is aangesteld en wie dat is. De gerechtvaardigde belangen van de bestuurder moeten kenbaar worden gemaakt. Ook moet er duidelijk zijn wie de ontvangers zijn van de persoonsgegevens. De bewaartermijn van de persoonsgegevens moet zijn aangegeven. De rechten die de betrokkene toekomen en er moet beschreven staan dat er een mogelijkheid is om een klacht in te dienen bij de AP.[121]

§ 4.3.3 Persoonsgegevensbeveiliging/beveiliging van de verwerking

Op grond van art. 32 AVG dient de verwerkingsverantwoordelijke een juiste beveiliging van de verwerking toe te passen. Er moet rekening worden gehouden met de stand van de techniek, de uitvoeringskosten, de aard, de omvang en de context van de verwerkingsdoeleinden. Er moet rekening worden gehouden met de risico's van de rechten en vrijheden van personen. Om dit te kunnen verwezenlijken, dient de verwerkingsverantwoordelijke passende, technische en organisatorische maatregelen te nemen ter beveiliging van de persoonsgegevens.[122] Dat de verwerkingsverantwoordelijke deze maatregelen moet nemen, vloeit tevens voor uit het algemene behoorlijkheidsbeginsel, integriteitbeginsel en vertrouwelijkheidsbeginsel. Onder technische maatregelen worden alle maatregelen verstaan die zonder menselijke ingrijpen een beveiligings- of toegangsaspect afdwingen. Met technische maatregelen wordt onder andere bedoeld de in de begrippenlijst genoemde 'pseudonimisering'. Het versleutelen van persoonsgegevens valt hier ook onder. Versleutelen houdt in dat gegevens zonder sleutel niet hersteld kunnen worden. Een toegangscontrole in de vorm van een gebruikersnaam en wachtwoord valt hier ook onder. Organisatorische maatregelen houdt in dat er regelingen worden getroffen met menselijk toezicht. Hierbij kun je denken aan een registratiesysteem dat bijvoorbeeld een bericht naar de manager stuurt bij ongebruikelijke handelingen door personeel.[123] Passende maatregelen houdt in dat de proportionaliteit in acht moet worden genomen. De genomen maatregelen moeten passen bij het doel van de verwerking. Aanvullend hierop bestaat er ook de plicht om de toezichthouder (AP) te informeren over inbreuken op de beveiliging.[124] Naast deze maatregelen bepaald de AVG dat er maatregelen dienen te worden genomen om de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van verwerkingssystemen en diensten te garanderen.

---

[119] 'Hoe ga je als verantwoordelijke om met het verwerken van persoonsgegevens onder de privacyverordening?', De privacycompany 2016, www.privacycompany.eu (zoek op *Hoe ga je als verantwoordelijke om met het verwerken van persoonsgegevens onder de privacyverordening*).
[120] 'Hoe ga je als verantwoordelijke om met het verwerken van persoonsgegevens onder de privacyverordening?', De privacycompany 2016, www.privacycompany.eu (zoek op *Hoe ga je als verantwoordelijke om met het verwerken van persoonsgegevens onder de privacyverordening*).
[121] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 75-78.
[122] J. Berkvens & C. Jakimowicz, Tekstuitgave Privacyverordening met geïntegreerde overwegingen, Wbp- en Richtlijn 95/46/EG-teksten en verwijstabellen, Den Haag: Boom juridisch 2016, p. 85.
[123] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 117.
[124] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 139-141.

Er dienen maatregelen te worden genomen, gericht op het tijdig kunnen herstellen van de beschikbaarheid van en de toegang tot persoonsgegevens bij een fysiek incident. Tot slot dient er vastgesteld te worden dat er procedures in gang moet worden gezet, om de doeltreffendheid van de genomen veiligheidsmaatregelen te garanderen.[125]

Certificering

In art. 32 lid 3 AVG wordt er gesteld dat een goedgekeurd certificeringsmechanisme, als bedoeld in art. 42 AVG, kan worden gebruikt om aan te tonen dat er maatregelen zijn getroffen om het beveiligingsniveau te waarborgen. Het mechanisme van certificering is een nieuw element geïntroduceerd door de AVG.[126] Om een betrokkene in staat te stellen snel het beschermingsniveau van hun privacy bij producten en diensten te laten beoordelen, heeft de AVG het mechanisme van certificering in het leven geroepen. Hierbij kan een verwerkingsverantwoordelijke via een certificeringsmechanisme een proces van verwerking, een middel voor verwerking of een daarbij ondersteunend middel zoals een beveiliging laten toetsen. Blijkt dit te voldoen aan de certificeringcriteria, dan mag men een bijbehorend zegel of merkteken voeren. Het gebruik van deze gecertificeerde technologieën en middelen dient met name ter versterking van het bewijs dat de verwerkingsverantwoordelijke zijn verplichtingen op grond van de AVG nakomt. Het nut van certificering is ook dat het kan worden gebruikt om aan te onderbouwen dat de gebruikte middelen voor verwerking voldoen aan Privacy by Design en Privacy by Default.[127]

Bewaren van persoonsgegevens

De AVG heeft ten opzichte van de Wbp, geen artikel opgenomen over de bewaartermijn. Dit wordt verweven in de beginselen van juistheid en opslagbeperking. Vast blijft staan dat organisaties persoonsgegevens niet langer mogen bewaren dan noodzakelijk is voor de verwezenlijking van de doeleinden waarvoor de persoonsgegevens verzameld zijn. De organisatie moet de gegevens vernietigen als ze niet meer nodig zijn voor het doel van het archief. Er geldt slechts één uitzondering dat gegevens bewaard mogen worden, indien de gegevens nodig zijn voor historische, statistische of wetenschappelijke doeleinden. De verantwoordelijke dient dan voorzieningen te treffen om te waarborgen dat de persoonsgegevens uitsluitend voor deze specifieke doeleinden worden gebruikt. De AVG stelt geen specifiek termijn voor het bewaren van persoonsgegevens. Er zou hier eventueel een andere wet op van toepassing kunnen zijn, bijvoorbeeld de Archiefwet.[128]

§ 4.3.4 Meldplicht datalekken

Er is sprake van een datalek als zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Bij een datalek gaat het om toegang tot of de vernietiging, de wijziging of het vrijkomen van persoonsgegevens, waardoor zij in handen kunnen zijn gevallen van derden die geen toegang tot die gegevens zouden mogen hebben. Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking. Voorbeelden hiervan zijn: het kwijtraken van een usb-stick, de diefstal van een laptop, een inbraak in een computersysteem door een hacker of het slordig omgaan met het beheer van wachtwoorden. Aangezien er bij de AVG een documentatieplicht geldt, is dit ook van toepassing op datalekken. Er dient een gestructureerd register te zijn dat in bezit van de organisatie moet blijven. Aangezien het register van de datalekken in bezit moet blijven van de organisatie, kan de AP elk moment dit register opvragen en controleren of er aan de meldplicht voor de datalekken is voldaan.[129] Een datalek dient op grond van art. 31 lid 1 AVG binnen 24 uur gemeld worden aan de AP. In de Wbp werd een termijn van 72 uur gehanteerd.

---

[125] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 138-140.

[126] MvT Uitvoeringswet AVG, p. 46.

[127] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 175.

[128] 'Bewaren van persoonsgegevens', www.autoriteitpersoonsgegevens.nl (zoek op *Bewaren van persoonsgegevens*).

[129] 'Voorbereiding op de Avg', Onderwerpen, AVG nieuwe Europese privacywetgeving, www.autoriteitpersoonsgegevens.nl/ (zoek op *voorbereiding op de AVG*).

In de AVG is er een extra eis gesteld aan de inhoud van de melding. In de melding dient de verantwoordelijke op te nemen welke maatregelen er worden getroffen om de negatieve gevolgen van de datalek te beperken. Ook moet er worden gemeld wat de aard van de inbreuk is, op welke betrokken categorieën de datalek invloed heeft en het aantal betrokkenen die door het datalek geraakt worden.

§ 4.3.5 Boetebevoegdheid AP

De AVG heeft de boetebevoegdheid flink uitgebreid ten opzichte van de Wbp. Alvorens een boete kan worden opgelegd, wordt door de AP eerst een corrigerende maatregel opgelegd. Deze corrigerende maatregel is een soort waarschuwing, maar ook een bevel tot uitvoeren van een specifieke plicht. Indien een aanwijzing wordt gegeven zal de AP aangeven welke wettelijke bepaling is overtreden en de overtreder opdragen om de overtreding binnen een bepaalde termijn te herstellen.[130] Is de overtreding opzettelijk of is er sprake van ernstige verwijtbare nalatigheid, dan kan er direct een boete worden opgelegd door de AP. Hierbij houdt de AP rekening met alle omstandigheden van het geval. Het maximale boetebedrag kan oplopen tot € 20.000.000 of vier procent van de totale wereldwijde jaaromzet. Indien er een boete wordt opgelegd dient er op grond van de AVG bij bepaling van de boete rekening te worden gehouden met:

- de aard, ernst en duur van de inbreuk;
- de opzettelijke of nalatige aard van de inbreuk;
- de genomen maatregelen om de schade van de cliënt te beperken.[131]

§ 4.4 Rechten van de betrokkene

Om de betrokkene te beschermen heeft de wet aan de betrokkene een aantal rechten toegekend. Deze rechten betreffen de zeggenschap van de betrokkene over zijn/haar persoonsgegevens. De AVG kent verschillende rechten toe aan personen van wie persoonsgegevens worden verwerkt. Deze rechten bieden meer middelen om de verwerking van hun persoonsgegevens te controleren en te beïnvloeden. Onderstaand worden de rechten van betrokkene opgesomd die onder de AVG worden aangevuld of uitgebreid:

Recht op informatie (artikel 13 en 14 AVG);

De organisatie moet de betrokkenen op de hoogte houden van het feit dat er verwerking plaatsvindt van zijn persoonsgegevens. Daarnaast moet het, tijdens het verzamelen van de persoonsgegevens en vóór de verwerking, voor de betrokkene duidelijk zijn wat de doeleinden van de verwerking zijn. Mocht het doel van de verwerking veranderen, dan moet de betrokkene daarover geïnformeerd worden.

Recht van inzage (artikel 15 AVG);

De verwerkingsverantwoordelijke moet de betrokkene de mogelijkheid geven om zijn of haar gegevens in te zien. De verantwoordelijke zal bij een inwilliging van het inzagerecht, de betrokkene moeten informeren over de in paragraaf 4.3.4. genoemde informatieverplichtingen.[132] Indien een verantwoordelijke vindt dat ten onrechte een beroep op het inzagerecht wordt gedaan, moet de verantwoordelijke aannemelijk maken op welke manier.[133] Geeft de verantwoordelijke aan dat er inderdaad persoonsgegevens worden verwerkt, dan dient er een volledig en begrijpelijk overzicht van de gegevens aan de betrokkene te worden verstrekt. Op grond van art. 15 lid 1 AVG dient ook een omschrijving van het doel of de doeleinden van de verwerking te worden gedeeld. Ook moeten de categorieën van gegevens waarop de verwerking betrekking heeft verstrekt worden. De ontvangers of categorieën van ontvangers van de gegevens moeten worden vermeld. De beoogde bewaartermijn moet vastgelegd zijn. De rechten van de betrokkene om te rectificeren of wissen moet worden medegedeeld. Er moet kenbaar worden gemaakt dat betrokkenen het recht heeft om een klacht in te dienen bij een toezichthoudende autoriteit.

---

[130] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 227.

[131] Artikel 6 Boetebeleidsregels Autoriteit Persoonsgegevens 2016, pag.1-4.

[132] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 85.

[133] ECLI:NL:RBGEL:2016:6691.

Wanneer de gegevens niet bij de betrokkene zelf zijn verzameld, dan de beschikbare gegevens over de bron van die gegevens, Tot slot moet er worden medegedeeld, indien van toepassing, dat er gebruik wordt gemaakt van geautomatiseerde besluitvorming.[134]

Recht op rectificatie (artikel 16 AVG);

Indien er onjuiste persoonsgegevens worden verwerkt heeft de betrokkene recht op rectificatie. Dit artikel is een uitwerking van het beginsel van juistheid van persoonsgegevens genoemd in paragraaf 4.2.2. Rectificatie houdt in dat er een aanvullende verklaring op basis van onvolledige gegevens kan worden ingediend. Een vereiste van rectificatie is dat deze direct moet plaatsvinden. De verwerkingsverantwoordelijke is verplicht iedere ontvanger aan wie persoonsgegevens zijn verstrekt in kennis te stellen van elke rectificatie, tenzij dit onmogelijk is of onevenredig veel inspanning vraagt.[135] De verwerkingsverantwoordelijke dient alle redelijke maatregelen te nemen om ervoor te zorgen dat onjuiste persoonsgegevens worden gerectificeerd.[136]

Recht op gegevenswissing/ vergetelheid (artikel 17 AVG);

De verwerkingsverantwoordelijke is verplicht persoonsgegevens van de betrokkene zonder onredelijke vertraging te wissen. Dit moet gebeuren als de persoonsgegevens niet langer nodig zijn voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt. De verwerkingsverantwoordelijke dient ook de gegevens te wissen als de betrokkene onverhoopt zijn toestemming intrekt en er geen andere rechtsgrond voor verwerking bestaat. De gegevens moeten ook gewist worden als betrokkene bezwaar maakt tegen de verwerking of als de persoonsgegevens onrechtmatig verwerkt zijn.[137]

Recht op beperking van de verwerking (artikel 18 AVG);

Het recht op beperking van de verwerking houdt in dat er (tijdelijk) niet verwerkt of gewijzigd mag worden. Mocht er een beperking zijn, dan moet de verwerkingsverantwoordelijke dit duidelijk in een bestand hebben aangegeven. Tevens moet de betrokkene op de hoogte worden gebracht van de beperking en ook als deze weer wordt opgeheven.[138]

Recht op overdraagbaarheid / dataportabiliteit (artikel 20 AVG);

De AVG heeft een nieuw recht geïntroduceerd namelijk het recht op dataportabiliteit. Betrokkene hebben het recht om haar of zijn persoonsgegevens op te vragen die hij aan de verantwoordelijke verstrekt heeft. Hierdoor ontstaat er voor betrokkene nog meer zeggenschap over zijn eigen persoonsgegevens. Een betrokkene heeft het recht om de gegevens van de verwerkingsverantwoordelijke te verkrijgen in gestructureerde, gangbare en machineleesbare vorm en heeft voorts het recht deze gegevens aan een andere verwerkingsverantwoordelijke over te dragen, zonder daarbij te worden gehinderd, tenzij dit afbreuk doet aan rechten en vrijheden van anderen. Het recht op overdraagbaarheid strekt zich enkel uit over gegevens die de betrokkene zelf heeft aangeleverd.[139]

Recht van verzet/bezwaar (artikel 21 AVG);

Betrokkenen hebben het recht om aan een organisatie te vragen hun persoonsgegevens niet meer te gebruiken. In de meeste gevallen is dit van toepassing op organisaties die de persoonsgegevens gebruiken voor marketingdoeleinden.

---

[134] A. Engelfriet, P. Kager & L. Meij, De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar, Amsterdam: Ius Mentis 2017, p. 86-87.

[135] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 89.

[136] J. Berkvens & C. Jakimowicz, Tekstuitgave Privacyverordening met geïntegreerde overwegingen, Wbp- en Richtlijn 95/46/EG-teksten en verwijstabellen, Den Haag: Boom juridisch 2016, p. 29.

[137] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 91.

[138] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 95.

[139] 'De AVG uitgelegd deel 5: accountability en documentatieplicht', News, www.nederlandict.nl/ (zoek op De *AVG uitgelegd deel 5: accountability en documentatieplicht*).

Indien de betrokkene bezwaar maakt dient de verwerkingsverantwoordelijke de verwerking te staken. Er zijn enkele uitzonderingen waarbij dit niet kan, dit zijn dan dwingende gerechtvaardigde gronden.[140]

§ 4.5 Privacy by Default en Design

Artikel 25 AVG bepaalt dat de verwerkingsverantwoordelijke zorg dient te dragen voor de privacygerichte ontwikkeling van haar producten en diensten. Veel organisaties maken gebruik van informatie- of registratiesystemen. De verwerkingsverantwoordelijke is verplicht om de standaardinstellingen zo in te richten dat alleen de persoonsgegevens die noodzakelijk zijn worden vastgelegd in deze systemen. Dit om het beginsel van minimale gegevensverwerking in acht te nemen. Het afstemmen van de standaardinstellingen op de bevoegdheden onder de AVG wordt Privacy by Default genoemd. Daarnaast wordt er gesproken over Privacy by Design. Dit houdt in dat er al in een vroeg stadium aandacht moet worden geschonken aan privacy. Het gaat hier voornamelijk over ICT-producten en –diensten. Er dient door de verwerkingsverantwoordelijke privacy-verhogende maatregelen te worden genomen.[141] Een voorbeeld van een privacy-verhogende maatregel is dataminimalisatie. Er worden bij dataminimalisatie zo weinig mogelijk persoonsgegevens verwerkt. Alleen de persoonsgegevens die noodzakelijk zijn om het doel te verwezenlijken, mogen worden verzameld en verwerkt. De in paragraaf 4.3.3. genoemde pseudonimisering is ook een privacy-verhogende maatregel.[142]

§ 4.6 DPIA (Data Privacy Impact Assessment)

Een DPIA (voormalig PIA) is een gegevensbeschermingseffectbeoordeling op grond van art. 35 AVG. In geval van verwerkingen met een hoog privacyrisico moet een DPIA worden uitgevoerd. Wanneer bijvoorbeeld op grote schaal bijzondere persoonsgegevens worden verwerkt, is het verplicht voor een organisatie om een DPIA uit te voeren. Door een DPIA worden vooraf de privacy-risico's van een gegevensverwerking in kaart gebracht.[143] Vanuit de in kaart gebrachte risico's worden maatregelen opgesteld om deze risico's te verkleinen.[144] Het uitvoeren van een DPIA helpt een organisatie om in kaart te brengen of de privacywetgeving van toepassing is en/of er op een juiste manier de wet wordt nageleefd. Indien uit de DPIA blijkt dat er een hoog risico rondom de verwerking van persoonsgegevens en er geen concrete maatregelen zijn getroffen door de verwerkingsverantwoordelijke, dan dient de verwerkingsverantwoordelijke vóór de verwerking, de AP raad te plegen.[145]

§ 4.7 FG (functionaris voor de gegevensbescherming)

Een functionaris voor de gegevensbescherming houdt intern toezicht of de privacywetgeving met betrekking tot verwerking van persoonsgegevens door organisaties wordt nageleefd. Niet alle organisaties zijn verplicht een functionaris voor de gegevensbescherming aan te stellen. In sommige gevallen is dit wel verplicht. Overheidsinstanties en publieke organisaties zijn altijd verplicht om een FG aan te stellen. Organisaties waarvan is vastgesteld dat gegevensverwerking als kernactiviteit kan worden aangemerkt, zijn ook verplicht om een FG aan te stellen. Daarnaast stelt de AVG een aantal eisen aan een FG. Een FG moet een natuurlijk persoon zijn die voldoende kennis heeft over IT, informatiebeveiliging van de organisatie en van de relevante privacywetgeving.[146]

---

[140] A.W. Duthler, A.J. Biesheuvel RA RE, Het Europees privacyrecht in beweging, Overzicht van actuele ontwikkelingen en mogelijke consequenties voor werkzaamheden van IT-auditors, februari 2013.
[141] Mr. C.W.J.M. Ebbers & dr. Ir. J, van Hoof & ir. C.E. Oude Weernink, *Privacyaspecten van track-en-tracetechnologie in de zorg*, p. 30.
[142] MvT Uitvoeringswet AVG, p. 45.
[143] Mr. C.W.J.M. Ebbers & dr. Ir. J, van Hoof & ir. C.E. Oude Weernink, *Privacyaspecten van track-en-tracetechnologie in de zorg*, p. 31.
[144] J. Berkvens & C. Jakimowicz, Tekstuitgave Privacyverordening met geïntegreerde overwegingen, Wbp- en Richtlijn 95/46/EG-teksten en verwijstabellen, Den Haag: Boom juridisch 2016, p. 93.
[145] J. Berkvens & C. Jakimowicz, Tekstuitgave Privacyverordening met geïntegreerde overwegingen, Wbp- en Richtlijn 95/46/EG-teksten en verwijstabellen, Den Haag: Boom juridisch 2016, p. 92.
[146] MvT Uitvoeringswet AVG, p. 104.

Ook moet een FG betrouwbaar zijn, hetgeen wordt geborgd door een geheimhoudingsplicht.[147] De positie van de FG wordt in art. 36 AVG omschreven. De AVG schrijft niet voor of een FG intern of extern wordt aangesteld. De FG dient zijn of haar taken en verplichtingen evenwel onafhankelijk te kunnen uitvoeren. Wanneer de FG echter naast zijn werkzaamheden als FG nog andere werkzaamheden vervult, dan is het wel zaak om zijn onafhankelijkheid in de uitoefening van de FG-taken goed te borgen.[148] Op dit gebied dient hij geen instructies te ontvangen over het uitoefenen van zijn functie. Hij moet er open voor staan om vaardigheden te ontwikkelen binnen de organisatie. Verder bestaan er voor de FG geen formele sanctiebevoegdheden. Door zijn controlerende bevoegdheid, rapporteert hij rechtstreeks aan het hoogste managementniveau.[149]

§ 4.8 De verwerkersovereenkomst (DPA)

De AVG biedt op grond van art. 28 AVG de mogelijkheid voor de verwerkingsverantwoordelijke, om een verwerker aan te stellen die ten behoeve van hem verwerkingen verricht. Een verwerker is een partij die persoonsgegevens verwerkt in opdracht van de verantwoordelijke, zonder aan zijn gezag te zijn onderworpen. Het gaat om een aparte persoon of instelling die wordt ingeschakeld. Er kan hierbij gedacht worden aan een extern ICT-bedrijf. In art. 28 AVG is opgenomen dat een verantwoordelijke alleen gebruik mag maken van een dienst van een verwerker, als deze verwerker voldoende garanties biedt dat de verwerking voldoet aan de AVG.[150] De bewerkersovereenkomst bestond al in de Wbp, maar hier worden nieuwe inhoudelijke eisen aan toegevoegd door de AVG. Er moet vooraf toestemming worden gevraagd aan de verantwoordelijke bij het inschakelen van subverwerkers. Ook dient de verwerker informatie ter beschikking te stellen aan de verantwoordelijke. Verder mag de verwerker niet zonder toestemming van de verantwoordelijke persoonsgegevens aan een derde partij verstrekken. [151] Tenslotte dient de verwerker na voltooiing van de verwerking ten behoeve van de verwerkingsverantwoordelijke, de persoonsgegevens terug te geven of te wissen.[152] Indien een verwerker zonder opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerkt, kan de verwerker worden aangemerkt als verwerkingsverantwoordelijke. De verwerker onder het gezag van de verwerkingsverantwoordelijke mag alleen handelen in opdracht van de verwerkingsverantwoordelijke op grond van art. 29 AVG.[153]

§ 4.9 Gegevensbeschermings- of privacybeleid

Uit art. 24 AVG vloeit voort dat de verantwoordelijke een gegevensbeschermings- of privacybeleid moet hanteren. Niet in alle gevallen is het opstellen van een dergelijk beleid verplicht. In dit beleid moeten de eisen uit de AVG worden aangegeven. De verantwoordelijke dient een omschrijving te geven van de categorieën persoonsgegevens die worden verwerkt. Er dient een beschrijving van de doeleinden te zijn waarvoor de persoonsgegevens worden verwerkt en wat de juridische grondslag daarvan is. Daarnaast dient te worden aangegeven hoe de organisatie aan de beginselen van verwerking van persoonsgegevens voldoet. Ook dienen de rechten van betrokkenen volledig te zijn opgesomd en hoe zij deze kunnen uitoefenen.

---

[147] 'Samenvatting Privacyverordening', *De privacycompany 2016*, www.privacycompany.eu (zoek op *Samenvatting Privacyverordening*).
[148] MvT Uitvoeringswet AVG, p. 49-50.
[149] Mr. I.P.V. van Schelven & Mr. P.C. van Schelven, Europese gegevensbescherming: van richtlijn naar verordening, p. 103.
[150] J. Berkvens & C. Jakimowicz, Tekstuitgave Privacyverordening met geïntegreerde overwegingen, Wbp- en Richtlijn 95/46/EG-teksten en verwijstabellen, Den Haag: Boom juridisch 2016, p. 80-81.
[151] www.autoriteitpersoonsgegevens.nl/ (zoek op: *verwerkersovereenkomst*).
[152] J. Berkvens & C. Jakimowicz, Tekstuitgave Privacyverordening met geïntegreerde overwegingen, Wbp- en Richtlijn 95/46/EG-teksten en verwijstabellen, Den Haag: Boom juridisch 2016, p. 81.
[153] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 125-134.

De verantwoordelijke dient passende maatregelen op te nemen in het beleid, om ervoor te zorgen dat de verwerking van persoonsgegevens in overeenstemming zijn met de AVG. Tot slot dient de organisatie aan te geven hoelang zij de persoonsgegevens bewaren.[154]

Privacy statement

Een privacyverklaring wordt ook wel een privacy statement genoemd. Dit is een informatief bericht die bijvoorbeeld op de website van een organisatie geplaatst kan worden. Dit behoort enerzijds tot een verplichting van de verwerkingsverantwoordelijke naar de betrokkene toe. Op grond van art. 13 AVG heeft de verwerkingsverantwoordelijke een actieve informatieplicht. Art. 13 AVG ziet op wanneer persoonsgegevens bij de personen zelf worden verzameld. Art. 14 AVG wordt buiten beschouwing gelaten, dit artikel ziet op wanneer persoonsgegevens niet van de betrokkene zelf zijn verkregen. Bij digitale diensten is het aan te raden om een privacyverklaring of een privacy statement te gebruiken. Alle benodigde informatie wordt dan op één plek aangeboden. De gevraagde informatie dient in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en duidelijk en eenvoudige taal verstrekt te worden.[155] Het informatief bericht moet de volgende gegevens bevatten op grond van art. 29 AVG Werkgroep:

- de identiteit van de verantwoordelijke moet kenbaar worden gemaakt;
- de doeleinden van de verwerking dienen vast te staan;
- de verplichting om gegevens te verstrekken;
- wie de ontvangers zijn van de gegevens;
- vermelding van eventueel gebruik van geautomatiseerde gegevensverzameling;
- de rechten van betrokkenen;
- de mate waarop het beveiligingsniveau is ingericht;
- een vermelding van de contactpersoon.

[154] 'Verantwoordingsplicht', Onderwerpen, AVG nieuwe Europese privacywetgeving, www.autoriteitpersoonsgegevens.nl (zoek op *Verantwoordingsplicht*).
[155] A. Engelfriet, P. Kager & L. Meij, De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar, Amsterdam: Ius Mentis 2017, p. 75-79.

5. Privacy binnen RADAR getoetst aan de AVG

In dit hoofdstuk wordt het privacybeleid, de wijze van informatieverstrekking en de daaruit vloeiende werkwijze getoetst aan de relevante bepalingen van de AVG. Het hoofdstuk zal de volgorde van hoofdstuk vier aanhouden.

§ 5.1 Toepasselijkheid AVG

De AVG is op grond van art. 2 lid 1 AVG van toepassing op iedere geautomatiseerde verwerking en bovendien op de niet-geautomatiseerde verwerking wanneer sprake is van een bestand. Wanneer er sprake is van verwerkingshandelingen via een ICT-middel of internet wordt dit gezien als een geheel of gedeeltelijk automatiseerde verwerking.[156] Bij RADAR worden persoonsgegevens verwerkt door middel van een geautomatiseerd systeem genaamd LBA-net. Dit systeem is online te raadplegen en hoeft niet te worden geïnstalleerd op een desktop of laptop. Vanuit dit systeem worden volledige cliëntdossiers opgebouwd met daarin verschillende persoonsgegevens verwerkt. Vrijwel iedere handeling kan worden gezien als een verwerking en vrijwel alle verwerkingen door RADAR betreffen persoonsgegevens die herleidbaar zijn tot individuele personen. De AVG is op grond van art. 3 lid 1 AVG van toepassing op de verwerking van persoonsgegevens in het kader van de activiteiten van een vestiging van een verantwoordelijke die in de Europese Unie plaatsvinden. RADAR is gevestigd in Nederland en behoort tot de Europese Unie, de AVG is om deze reden van toepassing op RADAR.

§ 5.2 De materiele normen voor rechtmatige verwerking

§ 5.2.1 Beginselen voor de verwerking

Persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. Het moet voor de betrokkene inzichtelijk zijn in hoeverre en op welke manier zijn of haar persoonsgegevens worden verwerkt. Dit dient dus bijvoorbeeld te worden verwerkt in de privacyverklaring die op de website staat, hetgeen nader zal worden toegelicht in paragraaf 5.4. Deze transparantie en duidelijkheid dient echter ook te bestaan bij andere communicatie zoals wanneer de betrokkene om inzage verzoekt of bij het afhandelen van een bezwaarschrift. RADAR biedt op dit moment onvoldoende transparantie ten aanzien van de verwerking van persoonsgegevens. Aan dit beginsel wordt dan ook niet voldaan. Voor cliënten is het onduidelijk op welke manier de persoonsgegevens worden verwerkt. Er is geen duidelijke handelswijze die elke klachtbehandelaar structureel aanhoudt. Uit de observaties en gesprekken is gebleken dat enkele klachtbehandelaars wel meedelen op welke manier de gegevensverwerking verloopt en anderen niet.[157] Het beginsel van doelbinding en minimale verwerking worden getoetst in paragraaf 5.6.

§ 5.2.2 Doeleinde en grondslag voor gegevensverwerking

De verwerking is alleen rechtmatig indien en voor zover aan ten minste één van de voorwaarden uit art. 6 AVG wordt voldaan. Uit de WGA komt de verwerkingsgrond van RADAR naar voren. In art. 1 sub a WGA wordt genoemd dat een ADV de taak heeft om burgers onafhankelijk bijstand te verlenen bij de afwikkeling van hun klachten gericht op discriminatie. In sub b wordt als kerntaak genoemd dat de klachten onder onderdeel a geregistreerd dienen te worden. De registratie en gegevensverwerking volgen door deze bepaling uit een wettelijke verplichting. Hieruit blijkt dat het noodzakelijk is dat zij persoonsgegevens verwerken om te voldoen aan een wettelijke verplichting die op RADAR als verwerkingsverantwoordelijke rust. Aangezien in art. 1 sub b WGA expliciet staat dat de klachten geregistreerd dienen te worden, mag ervan uit worden gegaan dat aan het beginsel van rechtmatigheid is voldaan.

§ 5.3 Verwerking persoonsgegevens

Binnen RADAR team klachtbehandeling worden er verschillende persoonsgegevens verwerkt. Welke gegevens worden verwerkt hangt af van de omstandigheden per klacht.

---

[156] HvJ EU 6 november 2003, zaaknr. C-101/01,Lindqvist.
[157] Zie bijlage VIII voor conclusie observaties en gesprekken.

Uit het verrichte onderzoek blijkt dat diverse persoonsgegevens worden verwerkt zoals vanzelfsprekend de NAW- gegevens. Daarnaast worden er ook bijzondere persoonsgegevens verwerkt op grond van de mogelijke discriminatiegronden. Hieronder worden de meest voorkomende persoonsgegevens getoetst op noodzakelijkheid.

Naam:

Voor de behandeling van klachten is het noodzakelijk om de naam van de cliënt te hebben. Het blijft mogelijk om een anonieme melding te doen, maar indien er een klacht wordt ingediend is het beschikken over een aantal persoonsgegevens van cruciaal belang. De verwantschap tussen het doel van de verwerking, namelijk het registreren van de klachten en het verlenen van bijstand, staat nauw in verband met het doel waarvoor de naam verwerkt wordt, namelijk contact opnemen en het aanspreken van cliënten. De naam van een cliënt wordt niet gezien als een gevoelig/bijzonder persoonsgegeven. Dit valt onder de algemene NAW-gegevens.

Adres:

Een woonplaats is noodzakelijk om de klacht in te delen per regio. Daarentegen is een adres alleen nodig om bijvoorbeeld post naar een cliënt toe te sturen. Post opsturen is een vorm van bijstand verlenen aan de cliënt. Hierdoor wordt het adres gezien als ter zake dienend en niet als bovenmatige verwerking. Mocht een cliënt aangeven dat hij/zij geen bemiddeling op prijs stelt, dan kan ervoor worden gekozen om het adres niet te verwerken. Er wordt dan ter plekke bijstand verleend, door bijvoorbeeld een luisterend te bieden en verdere verwerking van de persoonsgegevens is dan ook niet nodig. Daarnaast wordt een adres niet gezien als een gevoelig persoonsgegeven. Het mag worden verwerkt als de verwerking het doel van de organisatie dient.

Geboortedatum:

Bij de verwerking van persoonsgegevens bij een klacht wordt altijd een geboortedatum geregistreerd. Indien sprake is van discriminatie op grond van leeftijd, is het vanzelfsprekend noodzakelijk dat de geboortedatum wordt geregistreerd. Die kennis is dan van belang voor het doeleinde van het registeren van de klacht. Indien dit niet het geval is, rijst de vraag of verwerking van een geboortedatum wel ter zake dienend is of bovenmatig is.

Telefoonnummer en e-mailadres:

Een telefoonnummer en/of e-mailadres is nodig om contact op te nemen met de cliënt over de verdere verloop van de behandeling van zijn of haar klacht. Het doel is dan ook bijstand verlenen en sluit hierdoor nauw aan bij het verwerkingsdoel. Een telefoonnummer of een e-mailadres wordt niet gezien als een gevoelig persoonsgegeven.

Geslacht:

Het geslacht van een cliënt verwerken is noodzakelijk om het doel van de verwerking te realiseren. Het verlenen van bijstand aan een cliënt dient op een zorgvuldige wijze te gebeuren. Daar is het voor nodig om de cliënt aan te spreken met meneer of mevrouw. Ook wanneer er een klacht wordt ingediend op grond van geslachtsdiscriminatie, is het verwerken van het geslacht noodzakelijk. Om deze reden is het verwerken van het geslacht ter zake en dienend en niet bovenmatig.

§ 5.3.1 Verwerking van bijzondere categorieën van persoonsgegevens

Etnische afkomst/nationaliteit:

Etnische afkomst hangt nauw samen met het bijzonder persoonsgeven ‘ras’. Er wordt gerefereerd naar een nationaliteit of een geboorteland. Bij ras gaat het om gegevens waaraan de afstamming te herkennen is. Enkele klachtbehandelaars hebben tijdens observaties en gesprekken laten blijken dat het invullen van de herkomst geen verplicht veld hoort te zijn.[158] In het registratiesysteem wordt dit veld ‘herkomst’ genoemd.

De vraag rijst of bij elke klacht de herkomst ingevuld dient te worden. Het doeleinde, het verlenen van bijstand en het registreren van deze klachten, zou ook bereikt kunnen worden zonder dat bij elke klacht de herkomst wordt verwerkt. Door de gevoeligheid van een bijzonder persoonsgegeven moeten deze alleen verwerkt worden als het de strekking is van het doel.

[158] Zie bijlage IV voor observatie en gespreksverslag Rotterdam.

§ 5.3.2 Verwerking van discriminatiegronden

Overige discriminatiegronden:

De discriminatiegronden die genoemd zijn in paragraaf 3.3 mogen verwerkt worden als dat de strekking van het doel is. Om te bepalen of de te verwerken gegevens ter zake dienend zijn, moeten de klachtbehandelaars zich afvragen of zonder deze gegevens het doel kan worden bereikt. Het doeleinde is het verlenen van bijstand en registeren van klachten. Dat dit doeleinde niet bereikt kan worden zonder de discriminatiegrond te registeren is een voldoende nauwe verwantschap tussen het verwerkingsdoel en de te verkrijgen persoonsgegevens. Door de gevoeligheid van deze bijzondere persoonsgegevens mogen ze niet verwerkt worden buiten het doeleinde om. Als de klacht bijvoorbeeld is gericht op discriminatie op grond van godsdienst, is het relevant en noodzakelijk om ook te registeren op welk geloof de discriminatie gericht was. Uit bovenstaande informatie genoemd in paragrafen 5.3, 5.3.1, 5.3.2 blijkt dat RADAR de beginselen van doelbinding en minimale gegevensverwerking en opslagbeperking niet volledig in acht neemt. RADAR verwerkt meer persoonsgegevens dan noodzakelijk is om het doel te bereiken. De gegevens die verwerkt worden dienen ter zake dienend en beperkt te zijn tot wat noodzakelijk is om de doeleinden te bereiken.[159] Bij de verwerking dienen de beginselen van proportionaliteit en subsidiariteit tevens in acht te worden genomen. Uit de gegevensverwerking blijkt niet dat deze beginselen op een goede manier worden toegepast.

§ 5.3.3 Rechtvaardigingsgronden voor een rechtmatige verwerking van bijzondere persoonsgegevens

Het verwerken van bijzondere persoonsgegevens is verboden tenzij sprake is van een of meerdere rechtvaardigingsgronden. RADAR verwerkt bijzondere persoonsgegevens tijdens het registeren van de klacht. Hierbij kun je denken aan ras, nationaliteit, geloofsovertuiging en/ of handicap. Uit art. 9 lid 2 AVG volgen tien rechtvaardigingsgronden om deze gegevens toch wel te mogen verwerken. De eerste grond is de uitdrukkelijke toestemming. Hier wordt later op ingegaan in deze paragraaf. De rechtvaardiging op grond van een noodzakelijke verwerking ten aanzien van de uitvoering van verplichtingen op het gebied van arbeidsrecht of socialebeschermings- of socialezekerheidsrecht is op RADAR niet van toepassing. De in sub c genoemde vitale belangen zouden van toepassing kunnen zijn op RADAR. De bepaling wordt in zijn geheel ontkracht door de noodzakelijkheid, omdat de betrokkene fysiek of juridisch niet in staat zou kunnen zijn om toestemming te geven. Vervolgens zou de verwerking van bijzondere persoonsgegevens ook gerechtvaardigd zijn, wanneer dit door een vereniging, stichting of andere instantie zonder winstoogmerk gebeurt. Deze instanties moeten werkzaam zijn op het gebied van godsdienst, politiek of van een vakbond en de verwerking mag slechts betrekking hebben op de leden. Dit is voor RADAR niet van toepassing, zij verwerkt gegevens van cliënten en niet van leden. De volgende rechtvaardigingsgrond is dat de verwerking betrekking heeft op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt. Cliënten van RADAR hebben niet alle gegevens zelf openbaar gemaakt. Hierbij kun je denken aan persoonlijke gegevens die openbaar op sociale media zijn geplaatst. De volgende rechtvaardigingsgrond is gericht op verwerking die nodig is om een rechtsvordering te onderbouwen of uit te oefenen. Op RADAR is deze rechtvaardigingsgrond niet van toepassing. Zij verricht deze werkzaamheden niet. RADAR legt alleen zaken voor bij het CVRM. Hierbij wordt geen rechtsvordering onderbouwd of uitgeoefend. De rechtvaardigingsgrond die daarop volgt is, het verwerken in verband met arbeidsgeneeskunde of arbeidsgeschiktheid van een werknemer. Deze rechtvaardigingsgrond is tevens niet van toepassing op RADAR. Zij houdt zich bezig met discriminatie en niet met geneeskunde of arbeidsongeschiktheid. Ook de rechtvaardigingsgrond, de noodzakelijke verwerking voor het algemeen belang voor de volksgezondheid, is niet van toepassing op RADAR.

[159] A. Engelfriet, P. Kager & L. Meij, De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar, Amsterdam: Ius Mentis 2017, p. 41.

Zij heeft geen taken aangaande de volksgezondheid. De laatste rechtvaardigingsgrond is het verwerken van bijzondere persoonsgegevens vanwege historisch of wetenschappelijk onderzoek, archivering in het algemeen belang of statistische doeleinden op grond van een recht uit de lidstaat of van Unierecht. RADAR verwerkt bijzondere persoonsgegevens onder andere voor statistische doeleinden, namelijk het registreren van de klachten zodat aan het einde van het jaar een verslag kan worden uitgebracht met daarin de cijfers over discriminatie. Bij RADAR worden bijzondere persoonsgegevens echter ook verwerkt om bijstand te kunnen verlenen.[160] RADAR voldoet gedeeltelijk aan deze rechtvaardigingsgrond, maar omdat zij ook bijstand verleent kan dit niet worden geplaatst onder 'historisch of wetenschappelijk onderzoek, archivering in het algemeen belang of statistische doeleinden'. Daarnaast wordt er in artikel 27 Uitvoeringswet genoemd dat deze grond van toepassing kan zijn, als het vragen van uitdrukkelijk toestemming onmogelijk blijkt of dat het onevenredige inspanning zou vergen. Bij RADAR is dat niet het geval. Het is in de praktijk een extra handeling voor de klachtbehandelaars, maar deze vergt geen onevenredige inspanning.

Toestemming

RADAR voldoet niet geheel aan de voorwaarden, genoemd in sub a t/m j, op grond waarvan zij volledig zou kunnen zijn uitgesloten van de verplichting tot het vragen van uitdrukkelijke toestemming. Indien RADAR bijzondere persoonsgegevens wil verwerken, dient dan ook uitdrukkelijke toestemming te worden gevraagd aan de betrokken cliënt (art. 9 lid 2 sub a) Niet elke klacht die bij RADAR wordt ingediend, is gericht op een bijzonder persoonsgegeven. Enkel bij de klachten waar bijzondere persoonsgegevens worden verwerkt, dient vóór de verwerking hiervan uitdrukkelijke toestemming worden verkregen. RADAR moet aan kunnen tonen dat de betrokkene toestemming heeft gegeven voor het verwerken van zijn/ haar persoonsgegevens. Het blijkt uit observaties en gesprekken dat er op dit moment wordt volstaan met de redenering dat toestemming is gegeven doordat de cliënt RADAR zelf benadert.[161] Gelet op de werkwijze in de praktijk en meer gespecificeerd hoe een klacht wordt ingediend, blijkt dat er geen gebruik wordt gemaakt van toestemmingsvelden. Het klachtformulier bevat geen toestemmingsvelden. Telefonisch wordt niet om een uitdrukkelijk toestemming gevraagd of de gegevens verwerkt mogen worden. Dit geldt ook voor de wijze om via WhatsApp of e-mail een klacht in te dienen. Cliënten geven op geen enkele wijze uitdrukkelijk toestemming voor de gegevensverwerking.[162] Met de komst van de AVG geldt dat betrokkenen uitdrukkelijk toestemming dienen te geven voordat er mag worden overgegaan tot gegevensverwerking. Daarnaast is het belangrijk dat de betrokkene zich ervan bewust is waarvoor exact toestemming wordt gegeven (de te verwerken gegevens en de wijze waarop zij verwerkt worden). De betrokkene dient duidelijk voor ogen te hebben wat deze toestemming precies inhoudt. RADAR dient aan te kunnen tonen dat er toestemming is gegeven.

§ 5.3.4 Verstrekken gegevens aan derde(n)

Wanneer zich in de praktijk een intakegesprek voordoet, krijgt de wederpartij te horen welke persoon een klacht heeft ingediend. In paragraaf 5.3.2 is getoetst dat RADAR toestemming dient te vragen aan de betrokkene wanneer er bijzondere persoonsgegevens worden verwerkt. De informatie die verstrekt wordt aan de derde betreft de inhoud van de klacht en de persoonsgegevens van de melder. De inhoud van de klacht bevat de genoemde discriminatiegronden in paragraaf 3.3. Deze discriminatiegronden bevatten bijzondere persoonsgegevens en aangezien RADAR niet wordt uitgezonderd in de rechtvaardigingsgronden van art. 9 lid 1 AVG, dient toestemming te worden gevraagd aan de betrokkene voor verstrekking van deze gegevens. Wanneer RADAR persoonsgegevens wil verstrekken moeten deze op grond van art. 6 AVG verenigbaar zijn met het doel waarvoor ze verwerkt worden. RADAR's doel is om bijstand verlenen en om te bemiddelen met de wederpartij daarvoor is nodig om gegevens te verstrekken.

---

[160] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 59-64.
[161] Zie bijlage VIII voor conclusie observaties en gesprekken.
[162] Zie bijlage VIII voor conclusie observaties en gesprekken.

In het privacybeleid staat uitdrukkelijk vermeld dat de gegevens nooit zonder toestemming beschikbaar worden gesteld aan derden.[163] In de praktijk blijkt dat er geen structureel en/of schriftelijk toestemming gevraagd wordt aan betrokkene wanneer persoonsgegevens verwerkt worden noch om persoonsgegevens beschikbaar te stellen aan derden.[164]

§ 5.4 Verplichtingen verwerkingsverantwoordelijke

§ 5.4.1 Documentatieplicht

De documentatieverplichting uit de AVG houdt in dat een register wordt bijgehouden van de verwerkingsactiviteiten. Een dergelijk register moet worden bijgehouden als er minimaal 250 personeelsleden zijn of als er structureel verwerkingen van bijzondere persoonsgegevens plaatsvinden. Vrijwel alle klachten van RADAR zijn gericht op discriminatiegronden die ook bijzondere persoonsgegevens bevatten. Gelet hierop dient RADAR een register bij te houden. Team klachtbehandeling gebruikt in de praktijk een interne registratiewijze per regio. Voor de regio Rotterdam-Rijnmond en Zuid-Holland-Zuid wordt een fysieke registratielijst gehanteerd.[165] Voor de regio's Midden- en West-Brabant en Brabant-Noord bestaat een digitale lijst waarin alle klachten worden bijgehouden. Deze klachtregistratie kan worden gezien als verwerkingsactiviteiten. Buiten de aanmelddatum, naam van de cliënt, gemeente van de melder, plaats incident, omschrijving van de klacht, de klachtbehandelaar die de zaak behandelt en de vervolgstappen die genomen moeten worden, wordt niets in deze registratielijst benoemd. Hierdoor voldoet RADAR niet aan de documentatieplicht.

§ 5.4.2 Informatieplicht

RADAR dient de cliënt te informeren over de verwerkingsdoeleinden van de verzamelde persoonsgegevens. De informatieplicht wordt door de komst van de AVG fors uitgebreid. Naast de identiteit van de verantwoordelijke en de doeleinden van de verwerking, is RADAR door de komst van de AVG ook verplicht de contactgegevens van de FG, de rechtsgrond van de verwerking, de bewaartermijn van de gegevens en de rechten van de betrokkene mede te delen aan de betrokkene. Daarnaast is RADAR verplicht om aan de betrokkene te melden dat een eventueel gegeven toestemming kan worden ingetrokken, dat een klacht kan worden ingediend bij de toezichthouder, of de verstrekking van de gegevens verplicht is. Tevens is RADAR verplicht mee te delen wat de gevolgen zijn als de gegevens niet worden verstrekt en wat de kern van de taak-/rolverdeling is, indien meerdere partijen gezamenlijk verantwoordelijk zijn voor een verwerking. In de praktijk is het niet schriftelijk vastgelegd op welke manier dit in zijn geheel dient te gebeuren. RADAR heeft daarentegen wel een beknopte privacyverklaring op de website geplaatst.[166] Hieruit blijkt niet dat de bovengenoemde informatie wordt medegedeeld aan betrokkenen. Tevens blijkt uit observaties en gesprekken met klachtbehandelaars dat betrokkenen op dit moment nauwelijks geïnformeerd worden ten aanzien van de verwerking.[167] Om deze reden voldoet RADAR niet geheel aan de informatieplicht die zij hebben ten opzichte van de AVG.

§ 5.4.3 Beveiliging van de verwerking

Vanuit het algemene behoorlijkheidsbeginsel, integriteitbeginsel en vertrouwelijkheidsbeginsel is RADAR verplicht om passende technische en organisatorische maatregelen te nemen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Bescherming tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging van de persoonsgegevens moet de verantwoordelijke kunnen garanderen. RADAR gaat vanaf januari 2018 een nieuw registratiesysteem gebruiken.

---

[163] Zie bijlage II voor Privacybeleid RADAR, juni 2017.
[164] Zie bijlage VIII voor conclusie en observaties en gesprekken.
[165] Zie bijlage VIII voor conclusie observaties en gesprekken.
[166] 'Uw privacy', Read, www.radar.nl, (zoek op *uw privacy*).
[167] Zie bijlage VIII voor conclusie observaties en gesprekken.

De contactpersoon van RADAR team onderzoek en andere collega antidiscriminatiebureaus, georganiseerd in de brancheorganisatie LvtD (Landelijke vereniging tegen Discriminatie), zijn van mening dat het oude systeem geen goede beveiliging vertoonde.[168]
De AVG geeft aan dat pseudonimisering of het versleutelen van gegevens als twee belangrijke waarborgen worden gezien. In de praktijk blijkt dat deze twee middelen op dit moment allebei niet worden toegepast. Een andere belangrijke waarborg is een kwalitatief goede inrichting van de diensten en systemen waarmee de verwerking plaatsvindt. De contactpersoon van RADAR geeft aan dat het nieuwe systeem ‘’*Voldoet aan Wbp en OWASP top 10 volgens de overeenkomst die wij met de ontwikkelaar/bouwer hebben afgesloten”*.[169] Hieruit blijkt dat de huidige wet nog als uitgangspunt is genomen bij ontwikkeling van het registratiesysteem, en niet de AVG, die gewijzigde en aanvullende vereisten kent. In hoeverre aan de vereisten van de AVG, wordt voldaan is op dit moment niet duidelijk. Daarnaast blijkt uit de AVG dat certificeringsmechanismes kunnen worden gebruikt als element om aan te tonen dat passende technische en organisatorische maatregelen zijn getroffen. In de praktijk blijkt niet dat daar op dit moment gebruik van wordt gemaakt, of dat dit in de toekomst wel gaat gebeuren.

<u>Beveiliging fysieke dossiers</u>

RADAR maakt op één locatie nog gebruik van fysieke dossiers. In de meeste gevallen blijkt dat dossiers een papieren kopie van de digitale dossiers zijn. Een papieren kopie van een geautomatiseerde verwerking, zoals de dossiers uit het registratiesysteem, vallen onder het regime van die automatiseerde verwerking. Er kan gesteld worden dat een papieren kopie gelijk is aan het digitale dossier. De dossiers die RADAR print uit het registratiesysteem, kunnen hierdoor worden aangemerkt als geautomatiseerde verwerking die onder de AVG valt.[170] Dit betekent dat er passende technische en organisatorische maatregelen dienen te worden genomen, om de persoonsgegevens te beveiligen. In de praktijk blijkt dat de archieven openbaar en toegankelijk zijn. De kluis staat vrijwel de gehele dag open. Hieruit blijkt dat van optimale beveiliging niet gesproken kan worden. De gesloten dossiers worden in een kluis bewaard die wel afgesloten is en waarvan één medewerker de sleutel heeft.[171] RADAR heeft in haar privacybeleid opgenomen dat de medewerkers zorg moeten dragen voor privacygevoelige gegevens. De gegevens dienen op een vertrouwelijke wijze worden geadministreerd en gearchiveerd. Op dit moment voldoet RADAR nog niet aan haar eigen beleid.[172]

<u>Technische beveiliging</u>

In een interview met de contactpersoon van RADAR team onderzoek is gebleken dat het huidige registratiesysteem geen mogelijkheid biedt aan medewerkers om het wachtwoord te veranderen. Er wordt een standaard wachtwoord toegewezen. Er is tevens gebleken dat het nieuwe systeem dit ook niet automatisch gaat aanbieden. Er is wel voor gekozen om de medewerkers een eigen wachtwoord te laten instellen.[173] RADAR heeft in haar eigen privacybeleid opgenomen dat medewerkers alleen toegang hebben tot de klachten en meldingen van de vestiging waar zij werkzaam zijn.[174] In de praktijk blijkt dat klachtbehandelaars in elke regio kunnen inloggen en de klachten kunnen inzien.[175] Op dit gebied voldoet RADAR niet aan haar eigen beleid en aan de beginselen van integriteit en vertrouwelijkheid. Tevens is er in de praktijk geconstateerd dat desktops op de werkplekken niet vergrendeld worden wanneer klachtbehandelaars de werkplekken verlaten. Alle locaties van RADAR zijn toegankelijk voor buitenstaanders.

---

[168] Zie bijlage X voor interview contactpersoon RADAR.
[169] Zie bijlage X voor interview contactpersoon RADAR.
[170] A. Engelfriet, P. Kager & L. Meij, *De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar*, Amsterdam: Ius Mentis 2017, p. 15.
[171] Zie bijlage VIII voor conclusie observaties en gesprekken.
[172] Zie bijlage II voor privacybeleid, RADAR juni 2017.
[173] Zie bijlage X voor interview contactpersoon RADAR.
[174] Zie bijlage II voor privacybeleid, RADAR juni 2017.
[175] Zie bijlage VIII voor conclusie observaties en gesprekken.

Om de beveiliging van de dossiers en persoonsgegevens te waarborgen, dient de vergrendeling van deze persoonsgegevens optimaal te zijn. RADAR heeft in haar privacybeleid verschillende bepalingen opgenomen omtrent geheimhouding en vertrouwelijkheid. Zij heeft hiervoor een passende maatregel genomen om elke medewerker een geheimhoudingsverklaring te laten ondertekenen.[176] Om deze reden heeft RADAR aan het beginsel van behoorlijkheid voldaan. Uit een securityscan die RADAR heeft laten uitvoeren, in opdracht van verwerker Trends, is gebleken dat de e-mail beveiligd wordt met usernaam en wachtwoord. Trends maakt gebruik van digitale vertrouwde certificaten van Office 365 en Windows DC. Uit deze scan blijkt dat er geen Fronted scanning wordt uitgevoerd, maar office wel verdachte codes herkent. De lokale virusscanner werkt alleen op locatie, dus niet bij thuisgebruik.[177]

§ 5.4.4. Bewaartermijnen

Onder de documentatieplicht valt ook dat in het register moet staan welke bewaartermijnen worden gehanteerd. Aangezien één locatie van RADAR nog met papieren dossiers werkt, moet ook daarvoor een bewaartermijn vastgesteld worden. Het is de vraag in hoeverre het noodzakelijk is om dossiers te printen. Uit observaties en gesprekken is gebleken dat het voorkomt dat officiële stukken door cliënten per post worden toegezonden.[178] Hier geldt dat deze conform de nieuwe wetgeving gedigitaliseerd dienen te worden gelet op de beveiliging van de verwerking. Wat betreft de bewaartermijnen voor papieren en digitale dossiers heeft de AVG geen expliciete bepaling opgenomen. Uit gesprekken met klachtbehandelaars blijkt dat RADAR momenteel een termijn van vijf jaar hanteert voor de fysieke dossiers. Op grond van de archiefwet is dit een juiste termijn. RADAR heeft geen bewaartermijn geregeld voor de digitale dossiers. Bij steekproefsgewijze controle van het systeem is gebleken dat ook dossiers die langer dan vijf jaar geleden zijn gesloten, nog kunnen worden ingezien, waarbij eveneens nog alle persoonsgegevens zichtbaar zijn.[179]

§ 5.4.5 Meldplicht datalekken

Om betrokkenen bescherming tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging van de persoonsgegevens te garanderen, dient er een protocol meldplicht datalekken te zijn opgenomen. Een protocol geeft betrokkenen zekerheid en vertrouwen dat er op een juiste wijze gehandeld wordt indien er een datalek plaatsvindt. RADAR heeft nog geen protocol opgesteld omtrent de meldplicht datalekken. Uit een interview met een contactpersoon van team onderzoek blijkt dat er in de praktijk nooit sprake is geweest van een datalek. Het zou ook kunnen zijn dat RADAR de datalek niet heeft opgemerkt.[180] Ongeacht of in het verleden al eens sprake is geweest van een datalek, dient een protocol te worden opgesteld.

§ 5.5 Rechten van betrokkene

Met de komst van de AVG zijn de rechten van betrokkenen uitgebreider geformuleerd. RADAR heeft een aantal passages, gericht op de rechten van betrokkenen, opgenomen in het privacybeleid. Dit privacybeleid is niet voor cliënten en derden zichtbaar. In een aantal passages in het privacybeleid wordt nadrukkelijk besproken dat de cliënt wordt geïnformeerd over de wijze van dossiervorming. Daarnaast wordt in het privacybeleid genoemd dat cliënten recht op inzage in dossiers hebben.[181] Uit observaties en gesprekken blijkt dat er door klachtbehandelaars minimaal op de rechten van cliënten wordt gewezen. Voorts blijkt nergens uit dat de klachtbehandelaars het protocol klachtbehandeling verstrekken aan cliënten of er naar verwijzen.[182]

---

[176] Zie bijlage II voor privacybeleid, RADAR juni 2017.
[177] Zie bijlage IX voor offerte Constant-IT, laatste pagina.
[178] Zie bijlage VIII voor conclusie observaties en gesprekken.
[179] Zie bijlage VIII voor conclusie en observaties gesprekken.
[180] Zie bijlage X voor interview contactpersoon RADAR.
[181] Zie bijlage II voor Privacybeleid, RADAR juni 2017.
[182] Zie bijlage VIII voor conclusie observaties en gesprekken.

§ 5.6 Privacymaatregelen

§ 5.6.1 Privacy by Design & Privacy by Default

De begrippen Privacy by Design en Privacy by Default zijn van toepassing op de makers van het registratiesysteem (externe ICT-leveranciers). De beveiliging van de persoonsgegevens moet op een juiste wijze worden gerealiseerd bij het ontwerpen van de producten of diensten. In het geval van RADAR is dat het registratiesysteem. De organisatie en de makers van de systemen dienen technische en organisatorische maatregelen te nemen om de gegevens te beveiligen. Uit paragraaf 5.3 is gebleken dat meer persoonsgegevens verwerkt (kunnen) worden dan noodzakelijk voor de specifieke doeleinden van de organisatie. Het woord kunnen staat tussen haakjes, omdat het huidige systeem de mogelijkheid biedt om deze gegevens in te vullen.[183] Het huidige systeem bevat veel invulvelden en dropdownmenu's. Dit spoort medewerkers aan om gegevens in te vullen. In de praktijk blijkt dan ook dat het onduidelijk is welke velden ingevuld moeten worden.[184] Gelet op Privacy by Default dienen de standaardinstellingen van het systeem zo te worden ingericht dat dit niet mogelijk is. Omdat sprake is van te veel invulvelden, verwerkt RADAR onnodig bijzondere persoonsgegevens en wordt niet voldaan aan het beginsel van dataminimalisatie.

§ 5.6.2 DPIA (Data protection impact assessment)

Een DPIA is op grond van art. 35 AVG lid 7 vereist. In dit artikel staan een aantal gronden genoemd. RADAR voldoet aan de grond dat er op grote schaal bijzondere persoonsgegevens verwerkt moeten worden. Alle klachten die RADAR verwerkt zijn gericht op bijzondere persoonsgegevens. Op dit moment wordt bij elke klacht de etnische achtergrond van een cliënt geregistreerd.[185] Bij de registratie van een klacht worden de in paragraaf 3.3 genoemde discriminatiegronden altijd geregistreerd. Deze discriminatiegronden vallen onder bijzondere persoonsgegevens en zijn herleidbaar naar een identificeerbaar persoon. Op dit moment wordt er in de praktijk nog geen DPIA uitgevoerd, maar dit wordt wel verplicht voor RADAR.[186]

§ 5.6.3 FG (Functionaris voor de gegevensbescherming)

Een organisatie dient een FG aan te stellen indien er sprake is van een aantal gronden. Bij RADAR is er sprake van de laatste grond die wordt genoemd. Organisaties zijn verplicht een FG te benoemen als ze op grote schaal bijzondere persoonsgegevens verwerken en dit een kernactiviteit is. In de WGA staat genoemd dat de kernactiviteit van RADAR het verlenen van bijstand is, en dat deze klachten geregistreerd worden. Vrijwel alle geregistreerde klachten, gericht op discriminatie, kunnen worden gezien als bijzondere persoonsgegevens. De wet stelt een aantal eisen aan een functionaris voor de gegevensbescherming. In paragraaf 4.7 is uiteengezet aan welke eisen een FG moet voldoen. Dit kan niet getoetst worden aangezien RADAR geen FG heeft aangesteld.

§ 5.6.4 Verwerkersovereenkomst

In paragraaf 2.1.1 is het duidelijk geworden dat Cyriel Triesschijn, directeur/bestuurder van RADAR, de verwerkingsverantwoordelijke is. Hij heeft het doel en de middelen voor de verwerking van de persoonsgegevens vastgelegd. De verwerker daarentegen handelt overeenkomstig de instructies van de verwerkingsverantwoordelijke en onder diens uitdrukkelijke verantwoordelijkheid. Constant-IT heeft het huidige registratiesysteem gebouwd en in beheer. Doordat zij het systeem in beheer hebben dient er een verwerkingsovereenkomst gesloten te worden. In de praktijk zijn er geen verwerkingsovereenkomsten gesloten.[187] Dit geldt ook voor het nieuwe registratiesysteem.

---

[183] Zie bijlage X voor interview contactpersoon RADAR.
[184] Zie bijlage VIII voor conclusie observaties en gesprekken.
[185] Zie bijlage VIII voor conclusie observaties en gesprekken.
[186] Zie bijlage X voor interview contactpersoon RADAR.
[187] Zie bijlage X voor interview contactpersoon RADAR.

In de verwerkersovereenkomst wordt onder andere vastgelegd waar de persoonsgegevens voor mogen worden verwerkt en welke veiligheidsmaatregelen getroffen moeten worden waar de persoonsgegevens worden opgeslagen. De mogelijkheden om een audit uit te voeren en of de verwerker subverwerkers mag inschakelen voor de verwerking, wordt ook vastgelegd in de verwerkingsovereenkomst. Met de bouwer van het nieuwe registratiesysteem genaamd ‘Enigmatry’ is deze overeenkomst niet opgesteld.

§ 5.6.5 Gegevensbeschermingsbeleid

Organisaties zijn verplicht een gegevensbeschermingsbeleid op te stellen als dat in verhouding staat met de verwerkingsactiviteiten. De verplichting om een gegevensbeschermingsbeleid op te stellen, hangt af van de concrete omstandigheden. Zoals de aard, de omvang, de context en het doel van de gegevensverwerking. De verwerkingsactiviteiten van RADAR zijn gericht op het verwerken van bijzondere persoonsgegevens op grote schaal. Vrijwel alle klachten bestaan uit bijzondere persoonsgegevens, omdat ze gericht zijn op de discriminatiegronden. Het is voor RADAR verstandig om een gegevensbeschermingsbeleid op te stellen. RADAR heeft geen beschermingsbeleid opgenomen. Zij hebben wel een privacybeleid opgenomen, maar dit lijkt een privacyverklaring te zijn. De privacyverklaring op de website, te vinden in bijlage X, bevat niet de juiste informatie. Er moet in eenvoudige taal worden uitgelegd, wat er met de persoonlijke gegevens gedaan wordt.[188]

[188] Zie bijlage III voor informatieverstrekking, website RADAR.

6. Conclusies en aanbevelingen

In dit hoofdstuk zal de centrale vraag worden beantwoord. De centrale vraag luidt als volgt: ‘Welke aanbevelingen kunnen worden gegeven om het algemene privacybeleid en de werkwijze met betrekking tot de verwerking van persoonsgegevens door RADAR team klachtbehandeling zo aan te passen dat het privacybeleid en de werkwijze voldoen aan de Algemene verordening gegevensbescherming (AVG)?’.

6.1 Aanbevelingen die voortvloeien uit de toets van het beleid en de praktijk aan de AVG

Uit dit onderzoek blijkt dat bij RADAR geen goed beeld bestaat over haar verantwoordelijkheden en verplichtingen zoals neergelegd in de AVG. RADAR wil graag weten op welke punten zij tekortschieten in de uitvoering. Om de privacy van cliënten te kunnen waarborgen dient RADAR per 25 mei 2018 te voldoen aan de AVG. Er kan in het algemeen geconcludeerd worden dat er een aantal wijzigingen nodig zijn om in overeenstemming te werken met de AVG. In de volgende paragrafen worden er, per onderwerp uit de AVG, concrete aanbevelingen gegeven. De conclusies worden kort besproken, omdat daaruit de aanbevelingen voortvloeien.

6.1.1 De materiele normen voor een rechtmatige verwerking

Doeleinde en grondslag voor de verwerking

Uit dit onderzoek blijkt dat de grondslag voor de verwerking van persoonsgegevens voortvloeit uit de WGA. De registratie van de klacht en de gegevensverwerking volgt uit een wettelijke verplichting. Het doel van de verwerking is bijstand verlenen aan cliënten en het registeren van klachten. Er wordt RADAR aanbevolen om het doeleinde en de grondslag schriftelijk vast te leggen. Dit kan worden gerealiseerd door een gegevensbeschermingsbeleid op te stellen. Hier wordt verder op in gegaan in paragraaf 6.1.4.

Uitdrukkelijke toestemming voor verwerking van bijzondere persoonsgegevens

Uit mijn onderzoek van de praktijk blijkt dat RADAR uitdrukkelijke toestemming dient te vragen voor het verwerken van bijzondere persoonsgegevens. Uit observaties en gesprekken blijkt dat RADAR, op dit moment, geen toestemming vraagt voor de verwerking van deze bijzondere persoonsgegevens. RADAR dient deze uitdrukkelijke toestemming vóór de gegevensverwerking te ontvangen. Om deze reden wordt RADAR aanbevolen om dit in de praktijk toe te passen. Verder blijkt uit observaties en gesprekken dat er verschillende wijzen en middelen zijn om een klacht in te dienen. Het vragen van uitdrukkelijke toestemming kan in de praktijk werkbaar worden, door een toestemmingsformulier/button op de website te plaatsen. Indien klachten telefonisch worden ingediend, kan het bedrijfsbureau of de desbetreffende klachtbehandelaar, de cliënt verwijzen naar de website. De cliënt dient geïnformeerd te worden dat de toestemming geen vereiste is van de dienstverlening, maar dat het wel nodig is om bijvoorbeeld later te bemiddelen tussen partijen. Zie bijlage XVI voor een opgesteld toestemmingsformulier voor RADAR.

6.1.2 Verplichtingen verwerkingsverantwoordelijke

Verstrekken persoonsgegevens aan derde(n)

Uit onderzoek is gebleken dat de uitdrukkelijke toestemming, die is genoemd in bovenstaande paragraaf, ook van toepassing is op gegevensverstrekking aan derden. Uit observaties en gesprekken blijkt dat er aan cliënten geen expliciete toestemming, voor de gegevensverstrekking aan derden, wordt gevraagd. Naar aanleiding hiervan wordt er aanbevolen om een toestemmingsformulier/button voor de gegevensverstrekking aan derden te ontwerpen. Dit kan bijvoorbeeld door een elektronische toestemming op de website, die tegelijkertijd met de toestemming voor de gegevensverwerking kan worden gegeven. Er kan ook worden gekozen om deze toestemming apart of op een later moment te vragen. Op het toestemmingsformulier op de website kan dan een aparte bepaling worden opgenomen. De cliënt heeft hierdoor de mogelijkheid om later toestemming te verlenen, voordat wordt overgegaan op verstrekking van de persoonsgegevens. Dit is bijvoorbeeld realiseerbaar door een toestemmingsformulier in een e-mail te verstrekken.

Cliënt dient dit te ondertekenen, of toestemming te geven met een knop en de gegevens kunnen aan derden verstrekt worden.

Algemene documentatieverplichting

Uit mijn onderzoek is gebleken dat RADAR momenteel niet voldoet aan de documentatieplicht uit de AVG. RADAR wordt in principe vrijgesteld van het bijhouden van een register, omdat zij minder dan 250 medewerkers heeft. Echter levert de structurele verwerking van (bijzondere)persoonsgegevens risico's op voor betrokkenen. RADAR hanteert wel een interne registratiewijze. Uit gesprekken en observaties blijkt dat er, gelet op de registratiewijze, geen eenduidige werkwijze is. De aanbeveling aan RADAR luidt dan ook als volgt: 'gebruik één werkwijze binnen RADAR voor het registreren van de hoeveelheid klachten'. Dit kan bijvoorbeeld in een Excel-bestand waarin de klachten worden genummerd per regio, maar waar ook een totaal is te zien voor alle regio's. Zorg ervoor dat elke klachtbehandelaar deze kan raadplegen en hier ook mee gaat werken. Geadviseerd wordt om in elk intern overleg dit bestand te controleren op actualiteit. Met de bovenstaande aanbevelingen is er nóg niet voldaan aan de algemene documentatieplicht. Om aan de algemene documentatieplicht te voldoen, dient RADAR een register van verwerkingsactiviteiten op te stellen, waarin wordt aangetoond dat zij de juiste maatregelen hebben genomen om aan de AVG te voldoen. De bovenstaande aanbeveling voor het maken van een Excel bestand is ook van toepassing op dit register. Uit mijn onderzoek naar de praktijk, is naar voren gekomen dat de organisatie momenteel niet voldoet aan de documentatieplicht uit de AVG. Er wordt voor RADAR een opsomming gemaakt welke punten moeten worden opgenomen in een document, om aan de documentatieplicht te voldoen:

- de naam en contactgegevens van de verwerkingsverantwoordelijke;
- de verwerkingsdoeleinden;
- een beschrijving van de categorieën van cliënten en persoonsgegevens;
- de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt;
- de beoogde bewaartermijn;
- een beschrijving van de technische en organisatorische beveiligingsmaatregelen.

Beveiliging van de verwerking

Bewaartermijnen

Uit mijn onderzoek naar de praktijk is gebleken dat RADAR geen digitale bewaartermijn hanteert. De dossiers van langer dan vijf jaar geleden zijn volledig zichtbaar in het registratiesysteem. Dit betekent dat ook persoonsgegevens kunnen worden ingezien. Er wordt aanbevolen om een bewaartermijn op te nemen. Verder is uit mijn onderzoek gebleken dat RADAR een nieuw registratiesysteem krijgt. Met de makers van dit dergelijk registratiesysteem kan een digitaal bewaartermijn worden bepaald. De termijn van vijf jaar wat nu ligt voor de fysieke dossiers kan hierbij worden aangehouden. Indien het in de praktijk werkbaar is kan er vóór de termijn van vijf jaar gebruik worden gemaakt van de privacyverhogende maatregel 'versleuteling van persoonsgegevens' of 'pseudonimisering'.

Toegang en beveiliging

Uit een interview en gesprekken blijkt dat medewerkers toegang hebben tot alle dossiers van elke regio. In de offerte met de ICT-leverancier, die het registratiesysteem heeft ontwikkeld en momenteel beheerd, is vastgelegd dat medewerkers alleen toegang moeten hebben tot de regio waar ze werkzaam zijn. Er wordt aanbevolen om bij het nieuwe systeem dit weer in te voeren. Klachtbehandelaars moeten alleen toegang hebben tot het registratiesysteem van de regio waar zij werkzaam zijn. Om de privacy maximaal te waarborgen, moet er worden gekeken of het praktisch werkbaar is, om inzage in alle dossiers van de klachtbehandelaars te beperken tot haar eigen dossiers. Tevens is uit een interview met een contactpersoon van RADAR gebleken dat ze bij het huidige registratiesysteem een wachtwoord toegewezen krijgen. Op dit moment is er geen mogelijkheid om deze te veranderen. Wat betreft het toekomstig registratiesysteem wordt er wel een mogelijkheid aangeboden om het wachtwoord te veranderen. Er wordt aanbevolen om gebruik te maken van 'sterke wachtwoorden'.

Er zou ook gebruik kunnen worden gemaakt van tweestapsverificatie.
Dit betekent dat er een extra beveiliging wordt ingebouwd, waardoor je moet inloggen op twee manieren. Denk aan het inloggen bij de bank of DigiD. Er wordt dan ingelogd met een wachtwoord en er wordt een extra code naar bijvoorbeeld een telefoon gestuurd. Dit wordt tevens aanbevolen voor de toegang tot outlook. Als dit wordt ingevoerd hoeft RADAR zich geen zorgen te maken dat als ze bijvoorbeeld op een openbare computer inloggen hun wachtwoord via een keylogger wordt gestolen. Aangezien RADAR als organisatie veelal persoonsgegevens over de e-mail verstrekken en onderling delen is het essentieel om deze optimaal te beveiligen. Er wordt tevens aanbevolen om e-mailberichten die persoonsgegevens bevatten te versleutelen (encryptie). Dit kan gerealiseerd worden door een bepaalde abonnementsvorm van Office 365 af te nemen. Als er een e-mailbericht in Outlook versleutelt dan wordt de tekst omgezet in een code. Alleen de geadresseerde die beschikt over de persoonlijke sleutel waarmee het bericht is versleuteld, kan het bericht ontcijferen, zodat diegene het kan lezen. Een geadresseerde die niet over de bijbehorende privésleutel beschikt, ziet echter slechts ontcijferbare tekst. Hierdoor hebben klachtbehandelaars ook de mogelijkheid om veilig thuis (of op een andere locatie) te werken. Zie bijlage XI voor informatie over het gebruik van e-mail encryptie. Daarnaast is uit praktijkervaring gebleken dat medewerkers de desktop niet vergrendelen wanneer zij hun werkplek verlaten. Er wordt aanbevolen om dit onder de aandacht te brengen. Alle locaties van RADAR zitten namelijk gevestigd in kantoren waar bezoekers kunnen worden ontvangen. Verder is uit een interview gebleken dat RADAR een nieuw registratiesysteem aan het ontwikkelen is. De reden van de invoering van een nieuw registratiesysteem is, omdat in de praktijk blijkt dat de beveiliging van het oude systeem verouderd is. Hoewel RADAR voldoende maatregelen treft om de systemen optimaal te beveiligen, wordt er aanbevolen om te werken met certificering. Indien het nieuwe registratiesysteem gelanceerd is, kan na een periode de beveiliging worden getoetst. Blijkt RADAR aan de certificeringscriteria te voldoen, dan mag het een bijbehorend zegel of merkteken voeren. Daarnaast kan het gebruik van gecertificeerde technologieën en middelen het bewijs versterken dat RADAR de organisatorische en technische maatregelen uit de AVG is nagekomen.

Archief

In de praktijk blijkt door middel van observaties en gesprekken dat de archiefkluizen de juiste beveiliging hebben. Echter blijkt ook dat de kluis met het lopend archief vrijwel de gehele dag toegankelijk is. Om deze reden wordt aanbevolen de beveiliging van de fysieke dossiers te optimaliseren. Zorg ervoor dat de archiefkluis na elke handeling volledig wordt afgesloten. Mede gelet op enkele vorige aanbevelingen dient de opgestelde gedragscode voor medewerkers, te vinden in het privacybeleid, consequenter nageleefd te worden.

Meldplicht datalekken

Uit onderzoek naar de praktijk is gebleken dat bij RADAR nooit een datalek heeft plaatsgevonden en/of is opgemerkt in de praktijk. Om de juiste technische en organisatorische maatregelen te treffen dient RADAR een protocol meldplicht datalekken op te stellen. Er wordt aanbevolen om een protocol meldplicht datalekken op te stellen. Er kan ook voor worden gekozen om de maker van het toekomstige registratiesysteem, genaamd Enigmatry, een protocol datalekken te laten opstellen.

6.1.3 Informatieplicht en rechten van betrokkene

Uit juridisch onderzoek is gebleken dat de informatieplicht in de AVG flink wordt uitgebreid. Op dit moment worden cliënten van RADAR niet gewezen op de rechten die zij hebben. Uit observaties en gesprekken is gebleken dat er incidenteel op deze rechten wordt gewezen door klachtbehandelaars. Tevens blijkt uit de privacyverklaring op de website niet welke rechten de betrokkenen hebben. Er wordt geadviseerd om op de website een duidelijke privacyverklaring te plaatsen. Op de website moeten minimaal de volgende gegevens geplaatst worden in de vorm van een privacyverklaring:

- de identiteit van de verantwoordelijke;
- de doeleinden van de verwerking;
- in hoeverre het verplicht is om gegevens te verstrekken;

- ❖ wie de ontvangers zijn van de gegevens;
- ❖ vermelding van eventueel gebruik van geautomatiseerde gegevensverzameling;
- ❖ de rechten van de betrokkenen;
- ❖ het beveiligingsniveau;
- ❖ een vermelding van de contactpersoon.

6.1.4 Privacymaatregelen

Privacy by design en Privacy by default

Uit observaties en gesprekken blijkt dat RADAR onnodig bijzondere persoonsgegevens verwerkt, omdat de standaardinstellingen dit toelaten. Het registratiesysteem wekt de indruk dat bij elke klacht de herkomst van de cliënt moet worden ingevuld. Er staat namelijk een rode ster achter herkomst. Er wordt aanbevolen om het nieuwe registratiesysteem anders in te richten. Het is niet noodzakelijk om bij elke klacht alle (bijzondere) persoonsgegevens in te vullen. Het is raadzaam om klachtbehandelaars op de hoogte te stellen van wanneer er welke gegevens moeten worden ingevuld. In paragraaf 6.2 wordt er verwezen naar een stappenplan dat is opgesteld voor de klachtbehandelaars, om de privacy van de cliënten te waarborgen. Tevens blijkt uit mijn onderzoek dat alle digitale dossiers in te zien zijn, ook van langer dan vijf jaar geleden. Om deze reden wordt er aanbevolen om, gedurende het nieuwe registratiesysteem, de standaardinstellingen van het registratiesysteem, zo in te stellen dat afgesloten dossiers direct versleuteld of gepseudonimiseerd worden.

DPIA

Uit onderzoek naar de praktijk is gebleken dat RADAR op dit moment geen DPIA laat uitvoeren. RADAR is verplicht om een DPIA uit te voeren aangezien zij zich bezighouden met grootschalige verwerking van bijzondere persoonsgegevens. In een interview, met de contactpersoon van RADAR die zich bezighoudt met ICT-zaken, is naar voren gekomen dat ze er wel mee bezig zijn, maar dit nog niet gerealiseerd hebben. Door het uitvoeren van een DPIA wordt gekeken welke privacyrisico's van toepassing zijn voor RADAR. Daarnaast kan gekeken worden op welke wijze de privacyrisico's verminderd kunnen worden. Het wordt aangeraden om deze DPIA uit te voeren voordat het nieuwe registratiesysteem gelanceerd wordt. De privacyrisico's kunnen dan voor de gegevensverwerking in kaart worden gebracht. Eventuele maatregelen kunnen dan tijdig worden genomen om risico's te verkleinen. Dit kan bijvoorbeeld gerealiseerd worden door een externe beveiligingspexpert de DPIA te laten uitvoeren. Het is mogelijk dat de maker van het nieuwe systeem genaamd Enigmatry, zelf deze DPIA uitvoert. Het lijkt mij verstandiger om door een extern partij te laten beoordelen of het registratiesysteem voldoet aan de privacynormen gesteld in de AVG. Het registratiesysteem zal per januari 2018 in werking treden, mede gelet daarop wordt er aanbevolen om deze DPIA op een kort termijn te realiseren.

Functionaris voor de gegevensbescherming

Uit juridisch onderzoek is gebleken dat een FG verplicht is, indien de organisatie op grote schaal bijzondere persoonsgegevens verwerkt. Er kan gesteld worden dat bij RADAR hier sprake van is. Om deze reden wordt RADAR aanbevolen om een FG in dienst te nemen. Uit jurisprudentieonderzoek blijkt dat wanneer organisaties samenwerken, zij zelf kunnen bepalen of de FG binnen de organisatie wordt vastgesteld, of op landelijk niveau. Aangezien RADAR lid is van de landelijke antidiscriminatievoorzieningen, kan er worden gekozen voor een FG op landelijk niveau, of alleen binnen RADAR aan te stellen. Het voordeel van een FG binnen RADAR kan zijn dat de functionaris een betere kijk heeft op de gegevensverwerking. Daarnaast is de functionaris toegankelijker voor medewerkers om aan te spreken of advies te vragen. Een medewerker binnen RADAR kan functionaris voor de gegevensbescherming als neventaak hebben. Uit literatuuronderzoek blijkt dat een FG minimaal:

- ❖ kennis heeft van de nationale en Europese privacywet- en regelgeving over gegevensbescherming;
- ❖ begrip heeft van de gegevensverwerkingen die de organisatie uitvoert;
- ❖ begrip heeft van IT en informatiebeveiliging;
- ❖ kennis beschikt over de organisatie en de sector waarin die actief is;
- ❖ vaardigheden ontwikkelt om binnen de organisatie een cultuur van gegevensbescherming te ontwikkelen.

Verwerkersovereenkomsten

Uit interview met de contactpersoon van RADAR, die over ICT-zaken gaat, is gebleken dat RADAR geen verwerkersovereenkomsten heeft afgesloten met haar externe ICT-leveranciers. Uit onderzoek blijkt dat dit voor RADAR verplicht is, omdat zij verwerkers hebben ingeschakeld. RADAR dient met de verwerkers, op dit moment Constant-IT, vanaf januari 2018 wordt dat Enigmatry, een verwerkersovereenkomst op te stellen. In deze verwerkersovereenkomsten moeten duidelijke afspraken staan over op welke manier en hoe de persoonsgegevens worden beveiligd, de doeleinden voor de verwerking, de geheimhoudingsplicht en de meldplicht datalekken. Zie bijlage XIII voor een model verwerkersovereenkomst.

Gegevensbeschermings-privacybeleid

Uit juridisch onderzoek blijkt dat RADAR verplicht is om een gegevensbeschermingsbeleid op te stellen. RADAR heeft intern een privacybeleid opgesteld, maar dit lijkt op een privacyverklaring. De rechten van betrokkenen en de wijze van dossiervorming worden genoemd in dit intern privacybeleid. In bijlage XIV is een privacy statement opgesteld om op de website te plaatsen. Er wordt aanbevolen om het intern privacybeleid om te vormen naar een gegevensbeschermingsbeleid. In bijlage XV is er een opzet gemaakt voor een privacy-gegevensbeschermingsbeleid. Enkele bepalingen kunnen uit het huidige privacybeleid geschrapt worden en delen moeten herschreven worden. Er dient hier rekening te worden gehouden met de nieuwe bepalingen uit de AVG. Daarnaast wordt er aanbevolen om de opgestelde gedragscode, die zich in het huidige privacybeleid bevindt, consequenter na te leven. Er wordt met een gegevensbeschermingsbeleid bedoeld dat de organisatie kan laten zien dat zij aan de AVG voldoen. Uit jurisprudentieonderzoek blijkt dat in een gegevensbeschermingsbeleid minimaal de volgende gegevens moeten worden opgenomen:

- een omschrijving van de categorieën persoonsgegevens die verwerkt worden;
- een beschrijving van de doeleinden waarvoor de persoonsgegevens verwerkt worden en wat de juridische grondslag daarvan is;
- hoe er wordt voldaan aan de beginselen voor de verwerking van persoonsgegevens, zoals de verplichting om niet meer gegevens te verwerken dan noodzakelijk;
- welke rechten betrokkenen hebben en hoe zij die rechten kunnen uitoefenen. Zoals het recht om een klacht in te dienen bij de AP. Maar ook het recht op inzage, wijzigen, wissen en het ontvangen van alle geregistreerde gegevens;
- welke organisatorische en technische maatregelen de organisatie genomen heeft om de persoonsgegevens te beveiligen;
- hoe lang de persoonsgegevens worden bewaard.

6.2 Algemene aanbevelingen

Het is voor RADAR verstandig om de huidige en toekomstige medewerkers goed op de hoogte te brengen van het nieuwe beleid en de werkwijze in de praktijk. Aangezien er met de komst van de AVG veel gaat veranderen, is met name aan te raden om de medewerkers op de hoogte te brengen van deze wijzigingen. Om de organisatie een helpende hand te bieden, wordt er een presentatie gegeven over de veranderingen die de AVG met zich meebrengt. Deze presentatie is tevens terug te vinden in bijlage XI. Om de klachtbehandelaars een geheugensteun te bieden, tijdens de gegevensverwerking, is er een stappenplan ‘bewustwording van privacy voor klachtbehandelaars’ opgesteld. Dit stappenplan is terug te vinden in bijlage XII. Om het stappenplan altijd te kunnen raadplegen, kan ervoor worden gekozen om dit stappenplan in de vorm van een muismat of bureau-onderlegger aan te bieden. Op deze manier kunnen de klachtbehandelaars dit stappenplan altijd en op een gemakkelijke manier raadplegen. Tot slot wordt er aanbevolen om de medewerkers bewust te laten worden en bewust te laten blijven van de veranderingen rondom de privacywetgeving. Dit kan gerealiseerd worden middels cursussen en trainingen een aantal keer per jaar aan te bieden. Ook kan er gedacht worden aan een steekproef afname, om te controleren of de klachtbehandelaars de juiste stappen rondom privacy van de cliënt nemen.

Bronnenlijst

Boeken

Engelfriet, Kager & Meij 2017
A. Engelfriet, P. Kager & L. Meij, De Algemene Verordening Gegevensbescherming. Artikelgewijs commentaar, Amsterdam: Ius Mentis 2017.

Berkvens & Jakimowicz 2016
J. Berkvens & C. Jakimowicz, Tekstuitgave Privacyverordening met geïntegreerde overwegingen, Wbp- en Richtlijn 95/46/EG-teksten en verwijstabellen, Den Haag: Boom juridisch 2016.

Berkvens & Prins 2007
J.M.A. Berkvens & J.E.J. Prins, Privacyregulering in theorie en praktijk, Deventer: Kluwer 2007.

C. Arts 2016
C. Arts 2016, „Het accountability principe onder de Algemene Verordening Gegevensbescherming", consideratie augustus 2016.

Mr. J.M.A. Berkvens & Mr. S.M.M.C. Vinken & Mr. S.R. Wiegerinck & Mr. S.W.G. Wolters 2016
Prof. Mr. J.M.A. Berkvens, Mr. S.M.M.C. Vinken, Mr. S.R. Wiegerinck, Mr. S.W.G. Wolters Checklist Privacy, privacybeleid in 30 checklists, Van WBP naar AVG, Berghauser Pont; Publishing.

A.W. Duthler & A.J. Biesheuvel RA RE 2013
A.W. Duthler, A.J. Biesheuvel RA RE, Het Europees privacyrecht in beweging, Overzicht van actuele ontwikkelingen en mogelijke consequenties voor werkzaamheden van IT-auditors, Deventer: Uitgeverij Kluwer.

Fennel, Kroes, Koppejan & Thier 2016
S. Fennell, R. Kroes, F. Koppejan & A. Thier, *Privacy wetgeving inclusief de algemene verordening gegevensbescherming*, Oisterwijk: Wolf Legal Publishers 2016.

Hooghiemstra & Nouwt 2016
T.F.M. Hooghiemstra & S. Nouwt, *Sdu Commentaar Wet bescherming persoonsgegevens*, Den Haag: Sdu Uitgevers 2016.

J. Gerritsen 2015.
J. Gerritsen, „Waar gaat het heen met de avg", Informatie augustus 2015.

D.C. van Beelen & C.I.J. Klosterman & G. Noordeloos & P.L.F. Ribbers 2015
Privacy en gegevensbescherming, D.C. van Beelen, C.I.J. Klosterman, G. Noordeloos, P.L.F. Ribbers, Maklu: Apeldoorn-Antwerpen.

Parlementaire stukken

Arrest van het Hof van Justitie van de Europese Unie van 6 november 2003, C-101/01 (Lindqvist).

Kamerstukken II 2012/13 33 662, nr 3. Memorie van toelichting: Wet meldplicht datalekken.

Memorie van toelichting Uitvoeringswet Algemene Verordening Gegevensbescherming.

Rechtbank Gelderland, 304243, ECLI:NL:RBGEL:2016:6691.

Wetsvoorstel Uitvoeringswet Algemene verordening gegevensbescherming.

Handleidingen

Autoriteit Persoonsgegevens 2016.

Autoriteit Persoonsgegevens, Richtlijnen voor functionarissen voor de gegevensbescherming (FG's), 2016.

L.B. Sauerwein & J.J. Linnemann, 'Handleiding voor verwerkers van Persoonsgegevens (Wet bescherming persoonsgegevens)', Den Haag: Ministerie van Justitie 2002.

Tijdschriften

Mr. E. Oude Elferink & Mr. J.G. Reus, Handhaving van de Algemene Verordening Gegevensbescherming vanuit Nederlands perspectief, Boom: Kluwer 2017.

D.E. Comijs, Accountability in de AVG: betere processen en een sterkere positie van betrokkenen, Kluwer 2017.

De Jong, RegelMaat 2015, p. 6-18 J.P. de Jong, 'De Algemene verordening gegevensbescherming. De rechtsopvolger van de Wbp', RegelMaat 2015, afl. 1, p. 6-18.

Mr. C.W.J.M. Ebbers & dr. Ir. J, van Hoof & ir. C.E. Oude Weernink, Privacyaspecten van track-en-tracetechnologie in de zorg, Uitgeverij Parijs: Privacy en informatie 2017, p. 29.

G-J. Zwenne & L. Mommers, 'De tien belangrijkste veranderingen die de algemene verordening gegevensbescherming gaat brengen (in minder dan vijfduizend woorden)', Tijdschrift voor Compliance, 2016/4, p. 182-189.

Mr. I.P.V. van Schelven & Mr. P.C. van Schelven, Europese gegevensbescherming: van richtlijnnaar verordening, Boom: Juridisch tijdschriften 2016, afl. 3, p. 103.

Sikking, Vos & Zintel, Kennisnet 2015, p. 1-33 D. Sikking, J. Vos & C. Zintel, 'Privacy in 10 stappen', Kennisnet 2015, p. 1-33.

L.H. von Meijenfeldt, De AVG en Awb: vragen om Babylonische spraakverwarring, Uitgeverij Parijs: Privacy en informatie 2017, p. 124.

Elektronische bronnen

www.autoriteitpersoonsgegevens.nl bezocht, september 2017
www.consultancy.nl bezocht, oktober 2017
www.europadentraal.nl bezocht, september 2017
www.ictrecht.nl bezocht, oktober 2017
www.privacyscommission.be bezocht, december 2017
www.privacycompany.eu bezocht, oktober 2017
www.rijksoverheid.nl bezocht, september 2017