



De privacywaarborging van de patiënt

'Een onderzoek naar de inrichting en uitvoering van het extern privacybeleid van het VUmc conform de regelgeving van de AVG'

Toetsing van:

Afstudeeronderzoek

HBR-AS17-AS

Hogeschool Leiden	Opleiding HBO-Rechten
Naam student:	Anita Kroneman
Studentnummer:	S1087644
Afstudeerbegeleider:	Gerdo Kuiper
Onderzoeksdocent:	Maarten Verstuijf
Opdrachtgever:	VUmc: Marcel van der Haagen, Functionaris Gegevensbescherming
Inleverdatum:	13 juni 2018

Voorwoord

Geachte lezer,

Dit onderzoek is uitgevoerd in het kader van de afronding van mijn studie HBO-Rechten aan Hogeschool Leiden. In dit voorwoord wil ik mijn dank richten tot een aantal personen die het mij mogelijk hebben gemaakt om dit onderzoek uit te voeren.

Allereerst wil ik mijn opdrachtgever Marcel van der Haagen van het VUmc bedanken. Tijdens het zoeken naar een afstudeeropdracht ging mijn voorkeur uit naar een onderzoek binnen het gezondheidsrecht. Dit bleek echter een lastige opgave aangezien er nergens een plek beschikbaar was. Uiteindelijk is mijn vraag naar een afstudeeropdracht ter ore gekomen van de Functionaris Gegevensbescherming van het VUmc, Marcel van der Haagen, en heeft hij contact met mij opgenomen. Hoewel het geen onderzoek binnen het gezondheidsrecht betrof, heeft Marcel van der Haagen mij enorm enthousiast gemaakt over een onderzoek binnen het privacyrecht. Met heel veel plezier heb ik gewerkt aan dit onderzoek en ik wil Marcel van der Haagen dan ook bedanken voor het beantwoorden van mijn vragen en het ondersteunen van en meedenken met mijn ideeën.

Daarnaast wil ik mijn afstudeerbegeleider Gerdo Kuiper bedanken voor zijn hulp en begeleiding. Aangezien ik 26 april het eerste concept van mijn onderzoek moest inleveren bij mijn opdrachtgever ben ik direct heel hard aan de slag gegaan met het uitwerken van de theorie en het afnemen van interviews. Op een gegeven moment liep ik echter vast en heb ik de hulp van Gerdo Kuiper ingeschakeld. Dankzij hem heb ik weer een totaaloverzicht gekregen van mijn scriptie. Ik wil Gerdo Kuiper bedanken dat ik altijd terecht kon met mijn vragen en ook direct antwoord kreeg. Zonder deze hulp was het nooit gelukt om mijn onderzoek voor de deadline af te ronden.

Ook wil ik mijn afstudeerdocent Maarten Verstuijf danken voor de hulp tijdens het opstellen van mijn onderzoeksvoorstel en het mogelijk maken dat ik snel kon beginnen met mijn daadwerkelijke onderzoek.

Tot slot wil ik mijn beste vriendinnetje en huisgenootje Léonie danken voor de vele uren dat wij samen op de hogeschool hebben gewerkt, en voor de onvermoeibare steun die mij door de lange dagen heen hebben geholpen.

Ik wens u veel leesplezier toe.

Anita Kroneman

Leiden, 17 mei 2018

Samenvatting

Op 24 mei 2016 is de Algemene Verordening Gegevensbescherming (hierna: AVG) in werking getreden. Per 25 mei 2018 is deze verordening daadwerkelijk van toepassing in alle lidstaten van de Europese Unie. Met de invoering van de AVG verandert er veel voor organisaties. De AVG verplicht organisaties namelijk via diverse wegen zich te verantwoorden over de wijze waarop zij met persoonsgegevens omgaan.

Een onderdeel van deze verantwoordingsplicht is dat organisaties een extern privacybeleid dienen op te stellen en te presenteren aan betrokkenen. Het VUmc vraagt zich echter af hoe een dergelijk beleid moet worden ingericht en uitgevoerd. Het doel van dit onderzoek is dan ook om aan het VUmc aanbevelingen te doen wat betreft de inrichting en uitvoering van een extern privacybeleid conform de regelgeving van de AVG. In dit onderzoek is er daarom getracht een antwoord te geven op de volgende centrale vraag:

'Welk advies kan aan de hand van afgenomen interviews, analyse van wet- en regelgeving en literatuuronderzoek aan het VUmc worden gegeven over de inrichting van het extern privacybeleid en de praktische uitvoering daarvan, om voor 25 mei 2018 te voldoen aan de Algemene Verordening Gegevensbescherming?'

Het onderzoek is onderverdeeld in een literatuuronderzoek en een praktijkonderzoek. Bij het literatuuronderzoek is de AVG uitgebreid onderzocht en beschreven, is er gekeken welke veranderingen de verordening met zich meebrengt en welke punten van belang zijn voor het extern privacybeleid. Daarnaast is er onderzocht wat de AVG en Werkgroep 29 specifiek zeggen over de invulling van het extern privacybeleid. Uit dit onderzoek blijkt dat met name de verantwoordingsplicht en de informatieplicht een belangrijke rol spelen. Organisaties dienen transparant te zijn naar de betrokkenen toe en dienen hen helder en eenvoudig te informeren over de verwerking van hun persoonsgegevens. Om betrokkenen de zekerheid te kunnen bieden dat hun privacy goed gewaarborgd wordt, dienen organisaties allereerst een wettelijke grondslag hebben om persoonsgegevens te mogen verwerken. Daarnaast dienen zij zorgvuldig met persoonsgegevens om te gaan, onder meer door het nemen van technische en organisatorische maatregelen. Tevens dienen zij de rechten van de betrokkenen te respecteren en in acht te nemen. Wanneer dit op orde is kan een organisatie via het extern privacybeleid de betrokkenen informeren over de wijze waarop zij persoonsgegevens van betrokkenen verwerkt en hun privacy waarborgt. De AVG heeft aan het extern privacybeleid voorwaarden gesteld en Werkgroep 29 heeft hier nadere invulling aangegeven. Zo moet de informatie op een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal verstrekt worden. Daarnaast wordt er geadviseerd om een gelaagd privacystatement op te stellen.

Naar aanleiding van de punten die uit het literatuuronderzoek naar voren kwamen over de inrichting van het extern privacybeleid, is er praktijkonderzoek uitgevoerd, om te onderzoeken hoe deze regelgeving kan worden vertaald naar de praktijk van het VUmc. Het praktijkonderzoek is uitgevoerd door middel van het afnemen van interviews met een aantal medewerkers van het VUmc en AMC die direct of indirect betrokken zijn bij het opstellen en uitvoeren van het extern privacybeleid. De interviewvragen zijn gesteld aan de hand van de volgende topics:

1. Algemeen
2. Het extern privacybeleid onder de Wbp en onder de AVG
3. Communicatiekanalen extern privacybeleid
4. Uitvoering en toezicht extern privacybeleid

Door middel van het praktijkonderzoek is er gekeken naar hoe de bepalingen uit de AVG en de toelichting van Werkgroep 29 over de inrichting van het extern privacybeleid concreet kunnen worden toegespitst op het extern privacybeleid van het VUmc. Uit dit onderzoek kwam naar voren dat het met name van belang is om het extern privacybeleid aan te sluiten op alle patiëntendoelgroepen. Uit de interviews kwam naar voren dat dit kan door middel van een gelaagd extern privacybeleid dat in zeer eenvoudige taal is opgesteld en wordt ondersteund door aanvullende visualisatie. Uit de interviews kwam tevens naar voren dat het extern privacybeleid via verschillende communicatiekanalen aan patiënten moet worden bekend gemaakt. Tot slot kwam uit de interviews naar voren dat het van belang is dat er toezicht wordt gehouden op de medewerkers die de patiënten informeren over de verwerking van hun persoonsgegevens.

Naar aanleiding van het literatuuronderzoek en het praktijkonderzoek zijn er conclusies getrokken en zijn er aan het VUmc aanbevelingen gedaan met betrekking tot de inrichting en uitvoering van het extern privacybeleid conform de regelgeving van de AVG. Het belangrijkste is dat het VUmc wordt aanbevolen alle huidige losse informatie met betrekking tot privacy in te trekken en een volledig nieuw extern privacybeleid op te stellen. Tevens wordt aanbevolen om het nieuwe extern privacybeleid via verschillende kanalen te presenteren aan patiënten, onder meer via de website en via een folder. Er wordt aanbevolen om het extern privacybeleid te vertalen naar een beknopt, gelaagd privacystatement op de website, waar de informatie op een eenvoudige wijze, en in het Nederlands en Engels wordt gepresenteerd aan de patiënten. Daarnaast wordt er aanbevolen om werknemers een awarenessstraining te geven en toezicht te houden op de naleving van het extern privacybeleid door werknemers van het VUmc.

Inhoudsopgave

Samenvatting	3
Afkortingenlijst	7
Begrippenlijst	8
Hoofdstuk 1: Inleiding.....	9
1.1 Probleemanalyse.....	9
1.1.1 Aanleiding en context.....	9
1.1.2 Het praktijkprobleem	11
1.2 Doelstelling, centrale vraag, deelvragen	12
1.2.1 Doelstelling	12
1.2.2 Centrale vraag	12
1.2.3 Deelvragen.....	12
1.3 Onderzoeksmethode.....	13
Validiteit	16
Leeswijzer	16
Hoofdstuk 2: Achtergrond en ontwikkeling privacywetgeving	18
2.1 Ontwikkeling privacywetgeving	18
2.2 Privacywetgeving in de zorg	19
Hoofdstuk 3: De Algemene Verordening Gegevensbescherming.....	21
3.1 Achtergrond Algemene verordening Gegevensbescherming	21
3.2 Wettelijke grondslagen verwerken persoonsgegevens.....	24
3.3 Zorgvuldigheid	28
3.4 Technische en organisatorische maatregelen.....	30
3.5 Rechten van betrokkenen.....	31
3.6 Toezicht.....	33
Hoofdstuk 4: Het extern privacybeleid	35
4.1 Grondslag privacybeleid	35
4.2 Tweeledig beleid	35
4.3 Eisen extern privacybeleid	36
4.4 Inhoud extern privacybeleid	36

4.5 Vormgeving extern privacybeleid.....	38
4.6 Communicatiekanalen extern privacybeleid.....	39
4.7 Momenten van informatieverstrekking	40
Hoofdstuk 5: Het extern privacybeleid in de praktijk.....	42
5.1 Algemeen	43
5.1.1 Persoonsgegevens	43
5.1.2 Belang extern privacybeleid	46
5.2 Huidig en toekomstig extern privacybeleid	47
5.2.1 Huidig extern privacybeleid.....	47
5.2.2 Extern privacybeleid onder de AVG	51
5.3 Communicatiekanalen extern privacybeleid.....	51
5.3.1 Algemeen.....	51
5.3.2 Specifiek- Privacystatement	53
5.3.3. Specifiek- Folders	59
5.4 Uitvoering en toezicht extern privacybeleid	59
5.4.1 Uitvoering door medewerkers.....	59
5.4.2 Toezicht	61
Hoofdstuk 6: Conclusies en aanbevelingen	62
6.1 Conclusies	62
6.2 Aanbevelingen.....	65
Literatuurlijst.....	69
Bijlagen	

Afkortingenlijst

AMC	Academisch Medisch Centrum
AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
EVRM	Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden
Sr	Wetboek van Strafrecht
UAVG	Uitvoeringswet Algemene Verordening Gegevensbescherming
UVRM	Universele Verklaring van de Rechten van de Mens
VUmc	Vrije Universiteit medisch centrum
Wbp	Wet bescherming persoonsgegevens
Wet BIG	Wet op de Beroepen in de Individuele Gezondheidszorg
WGBO	Wet op de Geneeskundige Behandelingsovereenkomst

Begrippenlijst

Extern privacybeleid: In dit onderzoek wordt onder extern privacybeleid het volgende verstaan: Het beleid waarmee patiënten worden geïnformeerd over privacy binnen het VUmc. Dit beleid kan via diverse kanalen gecommuniceerd worden, waaronder via een privacystatement en folders.

Betrokkene: *'Degene van wie een organisatie persoonsgegevens verwerkt. Dit is dus degene op wie de persoonsgegevens betrekking hebben.'*¹ In dit onderzoeksrapport wordt met 'betrokkenen' de patiënten van het VUmc bedoelt.

Verwerkingsverantwoordelijke: Artikel 4 AVG *'Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.'* In dit onderzoeksrapport wordt met de 'verwerkingsverantwoordelijke' het VUmc bedoelt.

Werkgroep 29: Een onafhankelijk Europees advies- en overlegorgaan, samengesteld uit alle nationale privacytoezichthouders.² Per 25 mei 2018 is Werkgroep 29 overgegaan in de European Data Protection Board.³ In dit onderzoek zal echter nog worden gesproken over Werkgroep 29 omdat dit onderzoek vóór 25 mei is uitgevoerd.

¹Autoriteitpersoonsgegevens.nl (Zoek op: 'Wat zijn persoonsgegevens', onder het kopje 'Wie is de verwerkingsverantwoordelijke en wie is de betrokkene bij het verwerken van persoonsgegevens?') Geraadpleegd op: 11 april 2018

² Wijnant, 'Artikel 29-werkgroep publiceert richtlijnen voor begrippen van de Europese privacywet', *ictrecht.nl*, 2 januari 2017

³ Autoriteitpersoonsgegevens.nl (Zoek op: 'European Data Protection Board vandaag van start') Geraadpleegd op: 26 mei 2018

Hoofdstuk 1: Inleiding

Dit hoofdstuk is een inleiding op het uitgevoerde onderzoek. Allereerst wordt het probleem naar aanleiding waarvan dit onderzoek is uitgevoerd toegelicht. Vervolgens wordt de doelstelling van dit onderzoek, de centrale vraag en de deelvragen besproken. Daarna wordt er verantwoording afgelegd van de methoden die gebruikt zijn voor dit onderzoek en wordt de validiteit van dit onderzoek vastgesteld. Tot slot is er een leeswijzer aan dit hoofdstuk toegevoegd.

1.1 Probleemanalyse

1.1.1 Aanleiding en context

Privacy is hot topic. Iedere week komen er berichten in de media met betrekking tot privacy. Denk hierbij aan de 'facebook-affaire'⁴, het referendum over de 'Sleepwet' of de inzage in het dossier van Barbie door 85 medewerkers van het HagaZiekenhuis⁵.

Door deze berichten worden mensen steeds meer bewust van privacy en gaan ook actie ondernemen om hun eigen privacy te beschermen. Met de komst van de Europese Algemene Verordening Gegevensbescherming worden organisaties ook bewust gemaakt van het omgaan met de privacy van hun klanten, patiënten, cliënten of medewerkers. De nieuwe privacyverordening gaat dus een belangrijke positie innemen in de samenleving.

Op dit moment heeft iedere lidstaat van de Europese Unie (hierna: EU) nog een eigen privacywet. Deze nationale privacywetten zijn gebaseerd op de Europese richtlijn bescherming persoonsgegevens (95/46/EG) uit 1995. In Nederland is deze Europese privacyrichtlijn geïmplementeerd in de Wet bescherming persoonsgegevens (hierna: Wbp). De Wbp is op 1 september 2001 in werking getreden en is nog steeds van kracht.⁶

De Europese privacyrichtlijn werd dus vastgesteld toen het internet nog in de kinderschoenen stond en de wet daar nog niet op ingericht was.⁷ De afgelopen jaren zijn de toepassingsmogelijkheden van de informatietechnologie echter enorm ontwikkeld en zijn deze mogelijkheden ook grensoverschrijdend geworden. Het gevolg hiervan is dat persoonsgegevens over de gehele wereld uitgewisseld kunnen worden, zonder dat daar eenduidige wetgeving over bestaat. Doordat hier geen wetgeving over bestaat is de privacy van burgers in het geding gekomen.⁸

Nu de informatietechnologie dus grensoverschrijdend is geworden, is het van groot belang dat de privacywetgeving ook grensoverschrijdend wordt om zo vertrouwen te creëren in

⁴ S. Ephimenco, 'Wie om privacy geeft, moet vooral Facebook schreeuwend ontvluchten', Trouw 7 april 2018

⁵ F. Bouma, '85 medewerkers Hagaziekenhuis berispt na inbreuk dossier Barbie', NRC 26 april 2018

⁶ Autoriteitpersoonsgegevens.nl (Zoek op 'Wetten' onder het kopje 'Wet bescherming persoonsgegevens') Geraadpleegd op: 6 februari 2018

⁷ Autoriteitpersoonsgegevens.nl (Zoek op 'Wetten' onder het kopje 'Wet bescherming persoonsgegevens') Geraadpleegd op: 6 februari 2018

⁸ Matto, Baalbergen & Marouf, *De Algemene verordening gegevensbescherming en de gevolgen voor organisaties. Voor een duurzame digitale samenleving (white paper)*, advisor.nl, p. 1-3

gegevensbescherming via internet.⁹ Om deze redenen is de Europese privacywetgeving de afgelopen jaren herzien en is op 4 mei 2016 de Algemene Verordening Gegevensbescherming (hierna: AVG) gepubliceerd in het Publicatieblad van de Europese Unie. Met deze verordening geldt dus voor alle EU-lidstaten dezelfde privacywetgeving en wordt in iedere lidstaat de persoonsgegevens op dezelfde manier beschermd. De AVG is twintig dagen na publicatie in werking getreden, maar is pas vanaf 25 mei 2018 van toepassing. Tussen de inwerkingtreding van de AVG en het moment dat deze daadwerkelijk van toepassing is, zit dus een periode van twee jaar. Deze tijd is nodig om organisaties en toezichthouders zich goed te laten voorbereiden op de AVG. Tijdens deze twee jaar geldt in Nederland nog steeds de Wbp.¹⁰

Met de invoering van de AVG verandert er dus veel voor het VUmc. Patiënten krijgen meer mogelijkheden om voor zichzelf op te komen bij de verwerking van hun gegevens. Zo is het toestemmingsvereiste strenger geworden en zijn de privacyrechten van betrokkenen uitgebreid en versterkt.¹¹ Het belangrijkste recht wat nieuw is voor patiënten is het recht op dataportabiliteit. Dit recht houdt in dat patiënten het recht hebben om de persoonsgegevens te ontvangen die het VUmc van hen heeft. Die ontvangen gegevens moeten zij dan eenvoudig kunnen doorgeven aan bijvoorbeeld een ander ziekenhuis. Ook kunnen patiënten het VUmc vragen om gegevens rechtstreeks over te dragen naar het andere ziekenhuis.¹²

Naast de uitbreiding van de rechten van de patiënten, krijgt het VUmc ook meer verplichtingen bij het verwerken van persoonsgegevens. Zo legt de AVG in artikel 5 lid 2 meer nadruk op de verantwoordelijkheid van organisaties om aan te tonen dat zij zich aan de wet houden. Dit wordt ook wel de verantwoordingsplicht of accountability genoemd. Deze verplichting houdt in dat het VUmc op schrift moet kunnen aantonen dat zij de juiste organisatorische en technische maatregelen heeft genomen om aan de AVG te voldoen. Onder deze verantwoordingsplicht valt ook de transparantieplicht. Deze plicht is vastgelegd in lid 1 van artikel 5 AVG en houdt in dat het VUmc naar haar patiënten toe open dient te zijn over hoe zij met de verwerking van persoonsgegevens omgaat. Naast de verantwoordingsplicht is het VUmc op grond van artikel 35 AVG verplicht een Data Protection Impact Assessment (DPIA) uit te voeren. In het Nederlands wordt dit een gegevensbeschermingseffectbeoordeling genoemd. Dit is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen om vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.¹³ De derde nieuwe verantwoordelijkheid van het VUmc is dat zij op grond van artikel 37 AVG verplicht is een Functionaris voor de Gegevensbescherming (FG) aan te stellen. De Functionaris voor de Gegevensbescherming houdt binnen de organisatie toezicht op de toepassing en naleving van de AVG.

⁹ Europa-nu.nl (Zoek op 'Bescherming van persoonsgegevens in Europa') Geraadpleegd op: 8 februari 2018

¹⁰ Autoriteitpersoonsgegevens.nl (Zoek op: 'Algemene informatie AVG') Geraadpleegd op: 8 februari 2018

¹¹ Autoriteitpersoonsgegevens.nl (Zoek op: 'Algemene informatie AVG') Geraadpleegd op: 8 februari 2018

¹² Autoriteitpersoonsgegevens.nl (Zoek op: 'Rechten van betrokkenen' onder het kopje 'Vragen over het recht op dataportabiliteit') Geraadpleegd op: 8 februari 2018

¹³ Autoriteitpersoonsgegevens.nl (Zoek op: 'Data protection impact assessment (DPIA)') Geraadpleegd op: 8 februari 2018

Met de komst van de nieuwe privacyrechten van betrokkenen en de uitbreiding van de verantwoordelijkheden voor het VUmc kan het VUmc ook zwaarder gestraft worden als zij niet voldoet aan deze regelgeving. Wanneer het VUmc niet voldoet aan de AVG mag de Autoriteit Persoonsgegevens op grond van artikel 83 AVG een boete opleggen. Onder de Wbp waren deze boetes een stuk lager en was het toezicht ook minder streng. Voor het VUmc is het dus van groot belang dat zij zich houdt aan de regelgeving van de AVG.

1.1.2 Het praktijkprobleem

Het VUmc is op de hoogte van de veranderingen die de AVG met zich meebrengt. Op dit moment is zij echter nog niet voldoende voorbereid op deze verordening. Om hier verandering in te brengen heeft zij een gap-analyse uitgevoerd. Uit deze gap-analyse is gebleken dat het VUmc een aantal tekortkomingen heeft ten aanzien van de AVG. Het VUmc heeft derhalve op basis van het 10-stappenplan van de Autoriteit persoonsgegevens¹⁴ een plan van aanpak opgesteld met als concreet doel per 25 mei 2018 compliant aan de AVG de privacy van patiënten, onderzoeksdeelnemers, studenten en personeelsleden te beschermen. Het plan van aanpak bestaat uit zestien deelprojecten die bepaald zijn op basis van de uitkomsten van de gap-analyse. Een van deze deelprojecten is het wijzigen en inrichten van het extern privacybeleid conform de regelgeving van de AVG. Aangezien deze verordening vanaf 25 mei 2018 van toepassing is, is het voor VUmc van belang dat zij tijdig bruikbare aanbevelingen ontvangt om te zorgen dat ook het extern privacybeleid compliant is aan de AVG. Omdat de implementatie van alle aspecten van de AVG een zeer breed onderzoek betreft en het VUmc bij ieder deelproject een diepgaand onderzoek met bijbehorende gedetailleerde aanbevelingen opgeleverd wil zien, is mij gevraagd te focussen op deelproject 5 (Herzien intern en extern privacybeleid) en dan met name het extern privacybeleid, in samenhang met project 6 (Aanpassen voorlichtingsmateriaal betrokkenen). Aangezien in dit rapport dus twee van de zestien deelprojecten worden behandeld is het niet relevant om alle deelprojecten nog apart te benoemen, deze kunt u vinden in het Plan van Aanpak van het VUmc wat is opgenomen in bijlage I.

Zoals in de vorige paragraaf beschreven, krijgen patiënten op grond van de AVG meer privacyrechten. Patiënten hebben het recht om geïnformeerd te worden over hoe het VUmc aan de AVG voldoet. Vanaf 25 mei 2018 zal het VUmc aan de toezichthouder, de Autoriteit Persoonsgegevens, en aan haar patiënten hierover dan ook verantwoording af moeten leggen. Patiënten moeten weten hoe het VUmc met privacy omgaat, welke gegevens er worden verzameld en voor welke doeleinden registratie van persoonsgegevens nodig is. Het transparantieprincipe is derhalve het belangrijkste principe in de AVG. Om dit transparantieprincipe te waarborgen, is het VUmc verplicht een extern privacybeleid op te stellen en hiermee verantwoording over de verwerking van persoonsgegevens af te leggen

¹⁴ Autoriteitpersoonsgegevens.nl (Zoek op: 'In 10 stappen voorbereid op de AVG') Gedownload op: 9 februari 2018

aan haar patiënten. Aangezien het voor iedereen, ongeacht achtergrond, opleiding of IQ, duidelijk moet zijn hoe en waarom het VUmc persoonsgegevens verwerkt, heeft de AVG regels gesteld. Het privacybeleid moet begrijpelijk en transparant zijn voor iedereen en mag dus niet technisch of juridisch geformuleerd worden. Aangezien het VUmc op dit moment geen extern privacybeleid heeft, maar alleen een intern privacybeleid, ook wel Kaderregeling (Bijlage II) genoemd, is het voor het VUmc de uitdaging om een duidelijk en transparant extern privacybeleid op te stellen. Hoe zij dit het beste kan doen, moet door middel van gedegen onderzoek en concrete aanbevelingen blijken.

Ter verduidelijking van bovenstaande dient er te worden vermeld dat het extern privacybeleid van het VUmc niet slechts gericht is op patiënten, maar ook op onderzoeksdeelnemers en studenten. In dit onderzoek wordt er echter alleen aandacht besteed aan een privacybeleid voor patiënten aangezien het onderzoek anders te breed zou worden.

1.2 Doelstelling, centrale vraag, deelvragen

1.2.1 Doelstelling

Het doel van dit onderzoek is om op 26 april 2018 bij de heer Marcel van der Haagen, Functionaris Gegevensbescherming van het VUmc, een rapport in te leveren, waarin op basis van afgenomen interviews, analyse van wet- en regelgeving en literatuuronderzoek conclusies zijn getrokken en aanbevelingen worden gedaan over de wijze waarop het VUmc het extern privacybeleid moet inrichten en uitvoeren zodat het voldoet aan de Algemene Verordening Gegevensbescherming en hierdoor de privacyrechten van de patiënten van VUmc het beste worden gewaarborgd.

1.2.2 Centrale vraag

Uit de probleemstelling vloeit de volgende centrale vraag voort:

Welk advies kan aan de hand van afgenomen interviews, analyse van wet- en regelgeving en literatuuronderzoek aan het VUmc worden gegeven over de inrichting van het extern privacybeleid en de praktische uitvoering daarvan, om voor 25 mei 2018 te voldoen aan de Algemene Verordening Gegevensbescherming?

1.2.3 Deelvragen

Om tot een goede beoordeling van de centrale vraag te komen, zijn de volgende deelvragen opgesteld:

1. Wat kan er naar aanleiding van analyse van wet- en regelgeving en literatuuronderzoek worden gezegd over de inhoud van de Algemene Verordening Gegevensbescherming?

2. Wat kan er naar aanleiding van analyse van wet- en regelgeving en literatuuronderzoek worden gezegd over de wijzigingen die de Algemene Verordening Gegevensbescherming met zich meebrengt voor het VUmc ten opzichte van de Wet bescherming persoonsgegevens?
3. Wat kan er naar aanleiding van analyse van wet- en regelgeving en literatuuronderzoek worden gezegd over de eisen die de Algemene Verordening Gegevensbescherming stelt aan de invulling van het extern privacybeleid?
4. Wat kan er naar aanleiding van de interviews worden gezegd over de verwerking van persoonsgegevens en het belang van een extern privacybeleid binnen het VUmc?
5. Wat kan er naar aanleiding van interviews worden gezegd over de inrichting en uitvoering van het huidige extern privacybeleid en het toekomstige extern privacybeleid van het VUmc?
6. Wat kan er naar aanleiding van interviews worden gezegd over de communicatiekanalen waarmee het toekomstige extern privacybeleid van het VUmc, specifiek het privacystatement en folders, moeten worden verstrekt?
7. Wat kan er naar aanleiding van interviews worden gezegd over de uitvoering van en de toezicht op het toekomstige extern privacybeleid van het VUmc?

1.3 Onderzoeksmethode

Om een gedegen adviesrapport te kunnen schrijven is er goed en voldoende onderzoek nodig. Om dit onderzoek zo volledig mogelijk uit te voeren is er allereerst wetsanalyse en literatuuronderzoek uitgevoerd en is er vervolgens praktijkonderzoek uitgevoerd. Bij de wetsanalyse is er onderzoek gedaan naar relevante wet- en regelgeving met betrekking tot privacy in het algemeen en privacy in de zorg. Bij het literatuuronderzoek is er gebruik gemaakt van vakliteratuur, richtlijnen, kamerstukken en betrouwbare websites. Het praktijkgedeelte van het onderzoek is een kwalitatief onderzoek en is uitgevoerd door middel van het afnemen van half-gestructureerde interviews met medewerkers van het VUmc en AMC die direct of indirect betrokken zijn bij het opstellen en uitvoeren van het extern privacybeleid. In dit hoofdstuk zet ik per deelvraag uiteen welke onderzoeksstrategieën, bronnen en methoden er zijn gebruikt om de deelvragen te beantwoorden.

Het theoretisch-juridische onderzoeksgedeelte:

1. Wat kan er naar aanleiding van analyse van wet- en regelgeving en literatuuronderzoek worden gezegd over de inhoud van de Algemene Verordening Gegevensbescherming?

Bij de eerste deelvraag worden de juridische kaders uiteengezet en wordt er een grondige inhoudsanalyse van de AVG uitgevoerd.¹⁵ Dit is gedaan door middel van onderzoek naar rechtsbronnen en vakliteratuur. Daarnaast is er gebruik gemaakt van

¹⁵ In overleg met de opdrachtgever is ervoor gekozen om in dit onderzoek alleen de AVG te onderzoeken en niet tevens de UAVG, aangezien het onderzoek anders te breed zou worden.

wetenschappelijke artikelen uit het 'Tijdschrift voor Gezondheidsrecht' en het Nederlandse Juristenblad. Tevens is er gebruik gemaakt van de boeken 'Grondrechten' van J.H. Gerards e.a., 'Privacy in de zorg' van R. Huissen en 'Handboek gezondheidsrecht van H.J.J. Leenen e.a. Ook is er gebruik gemaakt van betrouwbare websites, waarbij de website van de Autoriteit Persoonsgegevens een grote rol speelt.

2. Wat kan er naar aanleiding van analyse van wet- en regelgeving en literatuuronderzoek worden gezegd over de wijzigingen die de Algemene Verordening Gegevensbescherming met zich meebrengt voor het VUmc ten opzichte van de Wet bescherming persoonsgegevens?

Voor de beantwoording van deze deelvraag zijn de voor dit onderzoek relevante bepalingen uit de AVG grondig geanalyseerd en er is een lijn getrokken naar de invloed die deze bepalingen hebben op het VUmc als zorginstelling. Om dit te kunnen beoordelen zijn de AVG en de Wbp naast elkaar gelegd om te onderzoeken welke veranderingen er zijn opgetreden. Tevens is er onderzocht wat er in de Wet op de Geneeskundige Behandelingsovereenkomst (WGBO) ligt vastgelegd over dit onderwerp en hoe dit zich verhoudt met de AVG. Daarnaast is er onderzocht wat de Europese Toezichthouders, de Artikel 29-werkgroep (hierna: Werkgroep 29), in haar richtlijnen heeft gezegd over de toepassing van de AVG. Daarnaast is er gebruik gemaakt van wetenschappelijke artikelen uit het Tijdschrift voor Gezondheidsrecht en het Nederlandse Juristenblad. Tevens is er gebruik gemaakt van de boeken 'Grondrechten' van J.H. Gerards e.a., 'Privacy in de zorg' van R. Huissen en 'Handboek gezondheidsrecht van H.J.J. Leenen e.a. Tot slot is er gebruik gemaakt van betrouwbare websites, waarbij de website van de Autoriteit Persoonsgegevens een grote rol speelt.

3. Wat kan er naar aanleiding van analyse van wet- en regelgeving en literatuuronderzoek gezegd worden over de eisen die de Algemene Verordening Gegevensbescherming stelt aan de invulling van het extern privacybeleid?

Bij deze deelvraag wordt er heel specifiek ingegaan op het onderwerp waar dit onderzoek op gericht is. Allereerst is de wettekst van de AVG geanalyseerd. Daarnaast is er onderzocht wat Werkgroep 29 in haar transparantierichtlijn heeft gezegd over de invulling van het extern privacybeleid. Tevens is er gebruik gemaakt van informatie van de website van de Nederlandse toezichthouder, de Autoriteit Persoonsgegevens. Tot slot is deze deelvraag nader onderbouwd door middel van een advies van een privacyadvocaat en een parlementair stuk met betrekking tot het extern privacybeleid

4. Wat kan er naar aanleiding van interviews worden gezegd over de verwerking van persoonsgegevens en het belang van een extern privacybeleid binnen het VUmc?

Voor het beantwoorden van deelvraag 4 zijn er interviews afgenomen met een aantal medewerkers van het VUmc en AMC die direct of indirect betrokken zijn bij het opstellen en uitvoeren van het extern privacybeleid. Aangezien de medewerkers op verscheidene vakgebieden deskundig zijn, zijn de interviewvragen deels aangepast aan het vakgebied en de deskundigheid van de betreffende medewerker. Met de volgende personen zijn er interviews afgenomen:

- Functionaris Gegevensbescherming VUmc, Marcel van der Haagen;
- Functionaris Gegevensbescherming en privacyjurist AMC, Marleen Inge;
- Stafadviseur Privacybescherming en Informatiebeveiliging VUmc, Wietske Ruiter;
- Privacyportefeuillehouder van de Cliëntenraad VUmc, Anat Fuldauer;
- Voorzitter van de Cliëntenraad VUmc, Paul Cohen;
- Directeur Medische Zaken AMC, Jan Drapers;
- Communicatieadviseur VUmc, Niels Jansen
- Medewerker Servicecentrum Zorgsupport VUmc, Jaap vermeulen;
- Businessanalist EVA Servicecentrum VUmc en AMC, Aage Hilbert

Hoewel dit onderzoek wordt uitgevoerd in opdracht van het VUmc, is er voor gekozen om interviews af te nemen met medewerkers van het VUmc en het AMC, daar het VUmc en AMC op termijn gaan fuseren en dus ook een gezamenlijk privacybeleid gaan hanteren. Het is daarom van belang om ook de kennis en ideeën van medewerkers van het AMC mee te laten wegen in dit onderzoek.

Voor de interviews is gekozen voor een half-gestructureerde methode. Voor het afnemen van elke interview is er een topic-lijst opgesteld met daarbij relevante open vragen die betrekking hebben op de deelvragen 4, 5, 6 en 7. Hierbij is de mogelijkheid opengelaten om door te vragen. Door het gebruik van deze methode kon er per participant een zo juist mogelijk beeld worden geschetst van de verwerking van persoonsgegevens binnen het VUmc, het belang van een extern privacybeleid en de inrichting en uitvoering van dergelijk beleid. In Hoofdstuk 5: Resultaten, is verantwoording afgelegd voor de keuze van de topics.

De methode die gebruikt is voor het beantwoorden van deelvraag 4, is eveneens van toepassing op de deelvragen 5, 6 en 7. Om onnodige herhaling te voorkomen is daarom bij deze deelvragen de methode niet nogmaals uitgewerkt. De deelvragen zijn hieronder wel nogmaals benoemd of verwarring te voorkomen.

5. **Wat kan er naar aanleiding van interviews worden gezegd worden over de inrichting van het huidige extern privacybeleid onder de Wbp en het toekomstige extern privacybeleid onder de AVG van het VUmc?**
6. **Wat kan er naar aanleiding van interviews worden gezegd over de communicatiekanalen waarmee het extern privacybeleid onder de AVG, specifiek het privacystatement en folders, moeten worden verstrekt?**
7. **Wat kan er naar aanleiding van interviews worden gezegd over de uitvoering van en de toezicht op het extern privacybeleid onder de AVG?**

Validiteit

Het theoretisch gedeelte van dit onderzoek is gebaseerd op wetsanalyse, literatuuronderzoek en onderzoek naar relevante richtlijnen en parlementaire stukken. Aangezien dit onderzoek draait om zeer recente wetgeving welke nog niet van toepassing is, is er gelet op de recentheid en betrouwbaarheid van bronnen. Onder recentheid wordt in dit onderzoek verstaan dat de informatie geschreven is over de Algemene Verordening Gegevensbescherming en niet over de Wet bescherming persoonsgegevens. De validiteit van het theoretische gedeelte is controleerbaar door raadpleging van de bronnen en literatuurverwijzingen.

Het praktijkgedeelte van dit onderzoek is gebaseerd op afgenomen interviews en documentanalyse. Zoals benoemd zijn deze interviews afgenomen met medewerkers van het VUmc en AMC die direct of indirect betrokken zijn bij het opstellen en uitvoeren van het extern privacybeleid. Aangezien de participanten op verscheidene vakgebieden deskundig zijn, zijn de interviewvragen deels aangepast aan het vakgebied en de deskundigheid van de betreffende participant, waardoor er een meer valide resultaat wordt behaald. Daarnaast is er van tevoren een proefinterview opgesteld en overlegd met de opdrachtgever, zodat de betrouwbaarheid van de vragen zijn getoetst. De validiteit van dit praktijkgedeelte is controleerbaar door raadpleging van de documenten en transcripties in de bijlagen.

Leeswijzer

Dit onderzoeksrapport is onderverdeeld in zes hoofdstukken. In hoofdstuk 1 wordt de aanleiding van het onderzoek, de centrale vraag en de deelvragen met methodische verantwoording beschreven. In hoofdstuk 2 wordt kort de achtergrond en de ontwikkeling van de (Europese) privacywetgeving beschreven en wordt er een lijn getrokken met de privacyregelgeving in de gezondheidswetten. In het hoofdstuk 2 wordt de Algemene Verordening Gegevensbescherming aan de hand van thema's en subthema's toegelicht en wordt er een vergelijking gemaakt met de huidige nationale privacywet, de Wet bescherming

persoonsgegevens. Hoofdstuk 4 gaat specifiek in op wat de Algemene Verordening Gegevensbescherming en de transparantierichtlijn van Werkgroep 29 zeggen over het extern privacybeleid. In hoofdstuk 5 zijn de resultaten van de afgenomen interviews uitgewerkt. In Hoofdstuk 6 worden uit deze resultaten conclusies getrokken en worden er naar aanleiding daarvan aanbevelingen gedaan. Tot slot zijn de literatuurlijst en de bijlagen opgenomen.

Hoofdstuk 2: Achtergrond en ontwikkeling privacywetgeving

Om een goed beeld te krijgen van de totstandkoming van de AVG wordt in dit hoofdstuk de ontwikkeling van de privacywetgeving in Europa en in Nederland besproken. Aangezien dit onderzoek uitgevoerd is in opdracht van het VUmc, wordt er in dit hoofdstuk tevens ingegaan op de positie van de AVG ten opzichte van bestaande privacywetgeving in de zorg.

2.1 Ontwikkeling privacywetgeving

Het recht op bescherming van persoonsgegevens maakt deel uit van het recht op eerbiediging van het privéleven, ofwel het recht op privacy. Het recht op privacy is een grondrecht, een klassiek vrijheidsrecht dat uitgaat van de bescherming van het individu op inbreuken van buitenaf op zijn privéleven.¹⁶ In artikel 12 van de Universele Verklaring van de Rechten van de Mens (hierna: UVRM) en in artikel 8 van het Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden uit 1950 (hierna: EVRM), ligt het recht op eerbiediging van het privéleven vastgelegd. Het recht op eerbiediging van het privéleven is uitgewerkt in het Dataprotectieverdrag van de Raad van Europa uit 1981. Dit verdrag heeft de basis gelegd voor de Europese privacybescherming en wordt ook wel Verdrag van Straatsburg of Conventie 108 genoemd. Het Dataprotectieverdrag heeft een wereldwijde reikwijdte. Ook staten die geen lid zijn van de Raad van Europa, kunnen het verdrag ondertekenen.¹⁷ In artikel 8 van het Handvest van de Grondrechten van de Europese Unie ligt heel specifiek het recht op bescherming van persoonsgegevens vastgelegd. In Nederland is het recht op privacy geregeld in artikel 10 van de Nederlandse Grondwet.

Hoewel er dus al verscheidene wetgeving bestond over privacybescherming kwam de eerste echte Europese privacyrichtlijn pas tot stand in 1995. Deze richtlijn is nog steeds van toepassing in de EU. Deze richtlijn heet voluit 'Richtlijn 95/46 van Het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens'. In Nederland is deze richtlijn geïmplementeerd in de Wet bescherming persoonsgegevens (hierna: Wbp). De Wbp trad in 2001 in werking en is momenteel nog van toepassing.¹⁸

Op 25 januari 2012 deed de Europese Commissie een voorstel voor een algemene Verordening voor gegevensbescherming. Er werd gekozen voor een nieuwe verordening in plaats van herziening van de oude richtlijn, om ervoor te zorgen dat er eenheid en harmonisatie in de bescherming van persoonsgegevens in heel de Europese Unie kwam. Een Europese *richtlijn* mag namelijk door lidstaten geïmplementeerd worden in eigen wetgeving.

¹⁶ Van der Jagt 2013, p. 22

¹⁷ Autoriteitpersoonsgegevens.nl (Zoek op: 'Internationale privacywetgeving') Geraadpleegd op: 19 februari 2018

¹⁸ Van Balen & Nijveld, Tijdschrift voor Gezondheidsrecht 2018, afl. 8, p. 608

Een Europese *verordening* werkt rechtsreeks door in nationale wetgeving, waardoor er voor iedere lidstaat dezelfde regelgeving geldt.¹⁹

Na een verloop van vier jaar is op 27 april 2016, twintig dagen na de bekendmaking van de AVG in het Publicatieblad van de Europese Unie, de AVG in werking getreden. Op grond van artikel 99 is de AVG echter pas op 25 mei 2018 van toepassing. In deze tussenperiode geldt de Europese privacyrichtlijn nog. Hierdoor krijgen organisaties de kans om zich voor te bereiden op de AVG.²⁰ Aangezien de Europese verordening rechtsreeks van toepassing is in alle lidstaten moeten daarnaast alle nationale privacywetten die gebaseerd waren op de Europese privacyrichtlijn worden ingetrokken. In Nederland wordt de Wbp ingetrokken en is de Uitvoeringswet Algemene Verordening Gegevensbescherming vastgesteld.²¹ Samen met de Europese richtlijn gegevensbescherming bij opsporing en vervolging zorgt de AVG voor een totale herziening van het gegevensbeschermingsrecht van de EU.

2.2 Privacywetgeving in de zorg

Naast de algemene wetten over privacy is er ook wetgeving specifiek gericht op privacy in de zorg. Op diverse manieren wordt de privacy van patiënten beschermd. Het beroepsgeheim ligt vastgelegd in artikel 457 van de Wet op de Geneeskundige Behandelingsovereenkomst (hierna: WGBO) en in artikel 88 van de Wet op de Beroepen in de Individuele Gezondheidszorg (hierna: Wet BIG). Het schenden van het beroepsgeheim is een strafbaar feit en wordt bestraft op grond van artikel 272 van het Wetboek van Strafrecht (hierna: Sr). Het beroepsgeheim geldt niet alleen voor de mondelinge communicatie tussen patiënt en zorgverlener, maar voor alle informatie die een zorgverlener binnen zijn beroep verzamelt. Hierbij gaat het dus ook om ziekenhuisopnames, verslagen van behandelingen, voorgeschreven medicijnen, maar ook privéomstandigheden en de gezinssituatie van de patiënt. Een hulpverlener mag alleen informatie van een patiënt met andere hulpverleners delen als deze hulpverleners betrokken zijn bij de behandeling. Wanneer een patiënt wordt doorverwezen naar een andere hulpverlener is voor het delen van medische gegevens aan die derde de toestemming van de patiënt nodig. Een patiënt moet door de hulpverlener uitdrukkelijk geïnformeerd worden over welke gegevens er gedeeld worden, voor welk doel deze gegevens gedeeld worden en waar die gegevens terechtkomen.²²

Ook voor het uitwisselen van medische gegevens op andere gebieden, onder meer via een zorgverzekeraar, geldt er strenge wetgeving. Ingevolge artikel 16 Wbp en artikel 9 AVG zijn gegevens over gezondheid 'bijzondere persoonsgegevens'. Op grond van deze artikelen is het dan ook verboden om deze gegevens te verwerken, omdat daarmee een inbreuk wordt gemaakt op de persoonlijke levenssfeer van burgers, welk recht we eerder bespraken.

¹⁹ Van Balen & Nijveld, Tijdschrift voor Gezondheidsrecht 2018, afl. 8, p. 608

²⁰ Van Balen & Nijveld, Tijdschrift voor Gezondheidsrecht 2018, afl. 8, p. 608

²¹ *De regelgeving voor de uitvoering van de AVG is te vinden op internetconsultatie.nl (zoek op 'Uitvoeringswet Algemene Verordening Gegevensbescherming').*

²² Huissen, 2015, p. 9

In 2016 is door de Eerste kamer het wetsvoorstel Elektronische gegevensuitwisseling in de zorg aanvaard. Deze wet, ook wel De wet Cliëntenrechten bij elektronische verwerking van gegevens genoemd, schept de randvoorwaarden waaronder medische gegevens veilig en elektronisch mogen worden uitgewisseld of ingezien. Daarnaast liggen in deze wet de rechten van cliënten bij elektronische gegevensuitwisseling vast.²³ Hierbij gaat het onder meer om het recht van de patiënt op elektronische inzage van zijn gegevens en de mogelijkheid om een elektronisch afschrift te ontvangen.²⁴

De komst van de AVG doet niets af aan de bestaande wet- en regelgeving over privacy in de zorg. Deze rechten en plichten blijven bestaan. De AVG is een aanvulling op de op de huidige privacywetgeving en zorgt ervoor dat de positie van individuen verstevigt wordt en de awareness onder organisaties vergroot wordt.²⁵

²³ Ministerie van Volksgezondheid, Welzijn en Sport, '*Elektronische gegevensuitwisseling in de zorg*', juni 2017

²⁴ Leenen e.a. 2017

²⁵ Autoriteitpersoonsgegevens.nl (Zoek op: 'Zorgverleners en de AVG') Geraadpleegd op: 22 februari 2018

Hoofdstuk 3: De Algemene Verordening Gegevensbescherming

In het vorige hoofdstuk is de ontwikkeling van de privacywetgeving in Europa en in Nederland, en de verhouding tussen de AVG en de bestaande privacywetgeving in de zorg besproken. In dit hoofdstuk wordt er nader ingegaan op inhoud van de AVG. Hierbij worden de punten besproken die van belang zijn voor de inrichting en uitvoering van het extern privacybeleid van organisaties. Allereerst wordt er wat meer achtergrondinformatie over de AVG gegeven. Vervolgens wordt er ingegaan op de wettelijke grondslagen voor het verwerken van persoonsgegevens, de vanuit de AVG gestelde zorgvuldigheidseisen en de te nemen technische en organisatorische maatregelen. Tevens worden de rechten van de betrokkenen besproken. Tot slot wordt er ingegaan op de toezicht die gehouden wordt op de naleving van de AVG.

3.1 Achtergrond Algemene Verordening Gegevensbescherming

Doelstelling

In artikel 1 van de AVG ligt het doel van de verordening vastgelegd. Het eerste doel van de AVG is het beschermingsniveau van persoonsgegevens verhogen door het versterken van de grondrechten en de fundamentele vrijheden van natuurlijke personen en dan met name het recht op bescherming van persoonsgegevens. In de vorige paragraaf hebben we gezien dat recht op bescherming van persoonsgegevens een grondrecht is. Verwerking van persoonsgegevens moet dan ook ten dienste staan van de mens. Het recht op bescherming van persoonsgegevens is echter geen absoluut recht. Het moet in evenredigheid worden afgewogen tegen andere grondrechten.²⁶

Het tweede doel, wat samenhangt met het eerste doel, is het teweegbrengen van een gelijkwaardig niveau van gegevensbescherming in alle lidstaten van de EU. Belemmeringen voor het vrije verkeer van persoonsgegevens binnen de Unie moeten worden opgeheven. Doordat de verordening in alle lidstaten van toepassing zal zijn, zal dit moeten bijdragen aan het vertrouwen in de digitale economie van de EU.²⁷

Toepassingsgebied

De AVG is net als de Wbp onderverdeeld in twee toepassingsgebieden. Het materieel toepassingsgebied, vastgelegd in artikel 2 AVG, en het territoriaal toepassingsgebied, vastgelegd in artikel 3 AVG.

De Wbp en de AVG zijn beide van toepassing op de geheel of gedeeltelijke geautomatiseerde bewerking van persoonsgegevens en op de persoonsgegevens die in een bestand zijn opgenomen of bestemd zijn om daarin opgenomen te worden. Het materieel

²⁶ De Vries & Goudsmit, Nederlands Juristenblad 2016/1077, afl. 22

²⁷ De Vries & Goudsmit, Nederlands Juristenblad 2016/1077, afl. 22

toepassingsgebied van de AVG is ten opzichte van de Europese privacyrichtlijn dus niet veranderd.²⁸

Het territoriaal toepassingsgebied is echter wel gewijzigd en ruimer geworden. Doordat het territoriale toepassingsgebied van de AVG ruimer is geworden kunnen bedrijven die niet onder de Wbp vielen, wel onder de AVG vallen. Dit houdt in dat zij dus ook verplicht zijn aan te tonen dat zij daadwerkelijk voldoen aan de privacywetgeving van de EU. Hiermee wordt de privacy van EU-burgers dus mondiaal beschermd.²⁹

Begrippen

In artikel 4 van de AVG staat een lijst begrippen uitgelegd die gebruikt wordt in de verordening. Een groot aantal van deze begrippen zijn hetzelfde als in de Europese Privacyrichtlijn. We bespreken de wijzigingen die van belang zijn voor dit onderzoek.

Het begrip 'persoonsgegevens' is verruimd aangezien er veel onduidelijkheid bestond over wat er precies onder 'alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon' werd verstaan. In considerans sub 26 van de AVG staat duidelijk uitgewerkt wat er precies onder 'identificeerbaarheid van een persoon' wordt verstaan.

Naast de wijziging van het begrip 'persoonsgegevens' zal er in de AVG niet meer gesproken worden over 'verantwoordelijke' maar over 'verwerkingsverantwoordelijke'. De betekenis van dit begrip blijft echter wel hetzelfde. Daarnaast is het begrip 'bewerker' veranderd in 'verwerker' en zal er voortaan niet gesproken worden over een 'bewerkingsovereenkomst' maar over een verwerkingsovereenkomst'. Ook deze veranderingen hebben geen impact op de betekenis van de begrippen.

Beginselen

Bij de verwerking van persoonsgegevens moet er op grond van artikel 5 AVG voldaan worden aan een aantal beginselen. In iedere sub van lid 1 van dit artikel is een beginsel uitgewerkt. Daarnaast is in lid 2 van dit artikel het belangrijkste beginsel vastgelegd.

Lid 1 sub a: Beginsel van rechtmatigheid, behoorlijkheid en transparantie

In de Wbp gold dit beginsel in feite ook al. Persoonsgegevens mochten ingevolge artikel 6 van de Wbp alleen verwerkt worden 'in overeenstemming met de wet'. Rechtmatig dus. Daarnaast moest de verwerking van de persoonsgegevens voor de betrokkene 'behoorlijk en zorgvuldig' zijn. Het begrip 'transparantie' is echter nieuw. De wetgever achtte het noodzakelijk dat dit begrip expliciet werd opgenomen in de wet. Op grond van dit beginsel zijn organisaties die onder de AVG vallen verplicht betrokkenen duidelijkheid te geven over de wijze waarop zij persoonsgegevens van betrokkenen verzamelt en verwerkt.

Het transparantieprincipe is in de AVG opgenomen omdat de AVG van organisaties die persoonsgegevens verwerken eist dat zij verantwoordelijkheid af kunnen leggen aan

²⁸ Essen, 'Het toepassingsgebied van de AVG, *solv.nl*, 27 juni 2016

²⁹ Essen, 'Het toepassingsgebied van de AVG, *solv.nl*, 27 juni 2016

betrokkenen. Deze plicht komt ook tot uiting in het accountabilityprincipe ³⁰, welke hierna zal worden behandeld.

Lid 1 sub b: Beginsel van doelbinding

Persoonsgegevens mogen alleen worden verzameld, verwerkt en gebruikt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden, en mogen vervolgens niet worden verwerkt op een andere wijze dan voor die doeleinden. Ingevolge artikel 13 AVG moet de betrokkene ook altijd geïnformeerd worden over deze doeleinden.

Lid 1 sub c: Beginsel van minimale gegevensverwerking

Alleen de persoonsgegevens die noodzakelijk zijn voor het doeleinde mogen worden verzameld, verwerkt en gebruikt.

Lid 1 sub d: Beginsel van juistheid

De organisatie moet er op toezien dat de gegevens juist zijn. Indien de persoonsgegevens onjuist zijn voor dat doeleinde moeten ze worden gewist of gerectificeerd.

Lid 1 sub e: Beginsel van opslagbeperking

Persoonsgegevens mogen na gebruik voor specifieke doeleinden slechts worden bewaard indien zij niet zorgen voor identificatie van de betrokkene.

Lid 1 sub f: Beginsel van integriteit en vertrouwelijkheid

De organisatie moet er op toezien dat de gegevens op een juiste technische en organisatorische wijze worden verwerkt zodat veiligheid gewaarborgd wordt en de persoonsgegevens tegen verlies, vernietiging of beschadiging beschermd worden.

Lid 2: Verantwoordingsplicht, Accountability-principe

De verantwoordingsplicht is de belangrijkste verplichting die de AVG oplegt aan organisaties. Middels deze verplichting legt de AVG veel nadruk op de verantwoordelijkheid van organisaties om aan te tonen dat zij zich aan deze wet houden.³¹ De verantwoordelijkheidsplicht omvat op grond van artikel 5 lid 1 AVG het naleven van alle beginselen die we hierboven bespraken. De organisatie moet haar verantwoordelijkheid nemen en kunnen aantonen dat haar verwerkingen voldoen aan de belangrijkste beginselen van rechtmatigheid, transparantie, doelbinding en juistheid.³² Daarnaast wordt de verantwoordingsplicht in artikel 24 AVG verder uitgebreid. Op grond van dit artikel moeten organisaties kunnen aantonen dat zij passende technische en organisatorische maatregelen hebben genomen om te waarborgen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd. Organisaties kunnen dit aantonen door bijvoorbeeld het opstellen en

³⁰ Nederlandict.nl (Zoek op: 'De Avg uitgelegd deel 2: transparantie en het recht op informatie') 8 maart 2017, Geraadpleegd op: 12 maart 2018

³¹ Autoriteitpersoonsgegevens.nl (Zoek op: 'Algemene informatie AVG' onder het kopje 'Algemene vragen over de AVG, 'Wat zijn de belangrijkste veranderingen voor organisaties?') Geraadpleegd op: 12 maart 2018

³² Autoriteitpersoonsgegevens.nl (Zoek op: 'Verantwoordingsplicht') Geraadpleegd op: 12 maart 2018

uitvoeren van een gegevensbeschermingsbeleid of een privacybeleid.³³ Aangezien alle verplichtingen van organisaties voortvloeien uit de verantwoordingsplicht, zal deze verplichting in dit onderzoek een rode draad zijn.

3.2 Wettelijke grondslagen verwerken persoonsgegevens

Iedere organisatie verwerkt persoonsgegevens. Artikel 6 van de AVG kent zes grondslagen voor het verwerken van persoonsgegevens:

- Toestemming van de betrokken persoon.
- De gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst.
- De gegevensverwerking is noodzakelijk voor het nakomen van een wettelijke verplichting.
- De gegevensverwerking is noodzakelijk ter bescherming van de vitale belangen.
- De gegevensverwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of uitoefening van openbaar gezag.
- De gegevensverwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen.

Dit wetsartikel is alternatief opgebouwd, wat inhoudt dat aan (minimaal) één van deze zes voorwaarden moet zijn voldaan om persoonsgegevens te mogen verwerken. Er hoeft dus niet aan alle voorwaarden worden voldaan. Organisaties zijn zelf verantwoordelijk om te beoordelen of zij aan een van deze voorwaarden voldoen.³⁴ Voor een organisatie is het echter wel van belang om te kunnen onderbouwen dat ze de verwerking van persoonsgegevens op een van deze grondslagen mag baseren. Dit vloeit voort uit de verantwoordingsplicht welke we eerder bespraken.

Toestemming

Eén van de grondslagen voor het verwerken van persoonsgegevens is 'toestemming'. Voor het verwerken van persoonsgegevens hebben organisaties op grond van artikel 6 lid 1 sub a AVG toestemming van de betrokkene nodig. Toestemming van de betrokkene wordt in artikel 4 lid 11 AVG gedefinieerd als *'elke vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee de betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling de hem betreffende verwerking van persoonsgegevens aanvaardt.'* De AVG geeft geen duidelijke omschrijving van de vorm waarop er toestemming moet worden gevraagd aan de betrokkene. De wijze waarop toestemming moet worden gegeven is wel aan een aantal eisen verbonden.

Artikel 7 AVG vereist dat organisaties kunnen aantonen dat ze ook daadwerkelijk toestemming van de betrokkene hebben ontvangen voor het verwerken van zijn

³³ Binnema & Frederiksz, 'AVG Deel III: Verwerker, verwerkingsverantwoordelijke en verwerkersovereenkomst', *europadecentraal.nl*, 5 maart 2018

³⁴ Autoriteitpersoonsgegevens.nl (Zoek op: 'Mag u persoonsgegevens verwerken?' onder het kopje 'Vragen over persoonsgegevens verwerken', 'Hoe weet u of u persoonsgegevens mag verwerken?') Geraadpleegd op: 12 maart 2018

persoonsgegevens. Toestemming moet dus expliciet worden gegeven. De Europese Unie geeft daarom in considerans sub 32 van de AVG aan dat *toestemming voor het verwerken van persoonsgegevens dient te worden gegeven door middel van een duidelijke actieve handeling. Dit kan bijvoorbeeld door een schriftelijke verklaring, ook met elektronische middelen, of een mondelinge verklaring, waaruit blijkt dat de betrokkene vrijelijk, specifiek, geïnformeerd en ondubbelzinnig met de verwerking van zijn persoonsgegevens instemt.* Impliciete toestemming voor het verwerken van persoonsgegevens is niet toegestaan. Een organisatie mag dus niet zomaar uitgaan van gegeven toestemming. Daarnaast is stilzwijgen, het gebruik van reeds aangekruiste vakjes of inactiviteit ook niet toegestaan. Artikel 7 AVG stelt tevens de eis dat toestemming even eenvoudig moet zijn als het geven daarvan.

Aangezien organisaties moeten kunnen aantonen dat er daadwerkelijk toestemming is verleend door de betrokkene, dienen zij zich er van te verzekeren dat de betrokkene zich ervan bewust is dat hij toestemming geeft en hoever deze toestemming rijkt. Considerans sub 42 van de AVG geeft aan dat er voor de aanvang van het verwerken van persoonsgegevens een verklaring van toestemming moet worden opgesteld. *Deze verklaring dient te worden verstrekt in een begrijpelijke en makkelijk toegankelijke vorm en in duidelijke en eenvoudige taal.* Om de betrokkene ook voldoende kennis van zaken te geven moet de organisatie de betrokkene tevens ten minste inlichten over de *identiteit* van de organisatie en de *doeleinden van de verwerking van de persoonsgegevens*.

Organisaties mogen zich dus op de grondslag 'toestemming' baseren wanneer de toestemming van de betrokkene aan deze besproken voorwaarden voldoet.

Uitvoering overeenkomst

Een organisatie mag de verwerking van persoonsgegevens op de grondslag 'uitvoering van een overeenkomst' baseren als zij een overeenkomst heeft met een betrokkene en hiervoor het verwerken van persoonsgegevens noodzakelijk is. De overeenkomst zelf mag niet gericht zijn op het verwerken van persoonsgegevens. Deze overeenkomst moet een ander doel hebben.³⁵

Wanneer een organisatie persoonsgegevens wil verwerken die niet direct noodzakelijk zijn voor de uitvoering van de overeenkomst, moet zij rechtsgeldige toestemming hebben van de patiënt of moet zij de verwerking op een andere grondslag kunnen baseren.³⁶

Wettelijke verplichting

Wanneer een organisatie zich wil baseren op deze grondslag zal het verwerken van de persoonsgegevens van patiënten noodzakelijk moeten zijn om te voldoen aan een wettelijke verplichting. In considerans sub 45 van de AVG wordt wel aangegeven dat de AVG *niet*

³⁵ Autoriteitpersoonsgegevens.nl (Zoek op: 'Mag u persoonsgegevens verwerken?' onder het kopje 'Vragen over grondslagen', 'Wanneer mag u zich baseren op de grondslag uitvoering overeenkomst?') Geraadpleegd op: 15 maart 2018

³⁶ Autoriteitpersoonsgegevens.nl (Zoek op: 'Mag u persoonsgegevens verwerken?' onder het kopje 'Vragen over grondslagen', 'Wanneer mag u zich baseren op de grondslag uitvoering overeenkomst?') Geraadpleegd op: 15 maart 2018

voorschrijft dat voor elke afzonderlijke verwerking specifieke wetgeving vereist is. In sommige gevallen is de verplichting voor het verwerken van persoonsgegevens namelijk niet expliciet opgenomen, maar is het wat ruimer geformuleerd. Een organisatie dient in dergelijke gevallen zelf te beoordelen of het verwerken van persoonsgegevens in die specifieke situatie noodzakelijk is om aan haar verplichting te voldoen.³⁷

Vitale belangen

Considerans sub 46 van de AVG geeft aan dat het verwerken van persoonsgegevens ook als rechtmatig dient te worden beschouwd *indien zij noodzakelijk is voor de bescherming van een belang dat voor het leven van de betrokkene of dat van een andere natuurlijke persoon essentieel is*. Voor een organisatie is een vitaal belang dus aan de orde in gevallen waarin het verstrekken van gegevens noodzakelijk is voor het leven of de gezondheid van een betrokkene en de betrokkene in een dergelijk geval niet meer in staat is zelf toestemming te verlenen. Op basis van de genoemde sub van de considerans mag een organisatie derden alleen toestemming geven tot medische gegevens die zij op basis van de grondslag vitale belangen verwerkt, indien zij de verwerking kennelijk niet op een andere rechtsgrond kan baseren.

Algemeen belang

Een organisatie kan zich alleen op deze grondslag beroepen indien zij een publieke taak uitoefent voor het algemeen belang of het openbaar gezag. Considerans sub 45 van de AVG geeft aan dat hieronder ook gezondheidsdoeleinden zoals volksgezondheid, sociale bescherming en het beheer van gezondheidszorgdiensten vallen. Organisaties zouden zich dus op deze grondslag kunnen beroepen indien zij de persoonsgegevens verwerken voor de uitoefening van een specifieke wettelijke taak. Voor de betrokkene moet het echter wel duidelijk zijn dat de organisatie zijn persoonsgegevens verwerkt voor de uitoefening van die specifieke wettelijke taak. Daarnaast dient de verwerking van de persoonsgegevens noodzakelijk te zijn om de publieke taak van de organisatie goed te kunnen vervullen.³⁸

Gerechtvaardigd belang

Een organisatie kan zich op deze grondslag baseren wanneer zij aan drie voorwaarden voldoet:

1. De organisatie heeft een gerechtvaardigd belang;
2. de verwerking is noodzakelijk om dit gerechtvaardigd belang te behartigen;
3. de organisatie heeft een afweging gemaakt tussen haar eigen belangen en de belangen van de betrokkenen waarvan zij persoonsgegevens verwerkt.

³⁷ Autoriteitpersoonsgegevens.nl (Zoek op: 'Mag u persoonsgegevens verwerken?' onder het kopje 'Vragen over grondslagen', 'Wanneer mag u zich baseren op de grondslag wettelijke verplichting?') Geraadpleegd op: 16 maart 2018

³⁸ Autoriteitpersoonsgegevens.nl (Zoek op: 'Mag u persoonsgegevens verwerken?' onder het kopje 'Vragen over grondslagen', 'Wanneer mag u zich baseren op de grondslag algemeen belang of openbaar gezag?') Geraadpleegd op: 16 maart 2018

1. Gerechtvaardigd belang

Ten eerste moet het gaan om een gerechtvaardigd belang. Dit belang moet volgens de Autoriteit Persoonsgegevens rechtmatig, voldoende duidelijk verwoord en ook echt aanwezig zijn.³⁹ Considerans sub 47 van de AVG geeft aan dat een dergelijk gerechtvaardigd belang bijvoorbeeld aanwezig kan zijn *wanneer sprake is van een relevante en passende verhouding tussen de betrokkene en de verwerkingsverantwoordelijke, in situaties waarin de betrokkene een klant is of in dienst is van de verwerkingsverantwoordelijke*. In geval van het VUmc zou het dus gaan om de verhouding VUmc en patiënt.

2. Noodzakelijkheid

Ten tweede moet de verwerking van de persoonsgegevens noodzakelijk zijn voor de behartiging van het gerechtvaardigde belang. De Autoriteit Persoonsgegevens geeft hierbij aan dat een organisatie de verwerking van persoonsgegevens dient te toetsen aan de eisen van proportionaliteit en subsidiariteit.⁴⁰ Op basis van considerans sub 47 van de AVG moeten organisaties daarom nagaan of de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene niet zwaarder wegen dan de verwerking. Het doel van de verwerking moet dus in verhouding staan tot de inbreuk voor de personen van wie de organisatie persoonsgegevens verwerkt (proportionaliteit), daarnaast moet er onderzocht worden of het doel niet op een voor de betrokken personen minder nadelige manier kan worden bereikt (subsidiariteit).⁴¹

3. Afweging belangen

Considerans sub 47 van de AVG geeft aan dat gerechtvaardigde belangen een rechtsgrond kunnen bieden voor verwerking, *mits de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene niet zwaarder wegen, rekening houdend met de redelijke verwachtingen van de betrokkene op basis van zijn verhouding met de verwerkingsverantwoordelijke*. Hiermee wordt bedoeld dat dat organisaties een goede afweging moeten maken tussen de belangen van de betrokkene van wie zij persoonsgegevens verwerkt en haar eigen belangen. Dit heeft onder meer te maken met de bewaartermijn van persoonsgegevens. Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk is voor het doel van de verwerking. Gaat het bijvoorbeeld om de verwerking van persoonsgegevens van kinderen onder de 16 jaar? Dan weegt het gerechtvaardigd belang van de organisatie minder snel op tegen de rechten en vrijheden van deze kinderen.⁴²

³⁹ Autoriteitpersoonsgegevens.nl (Zoek op: 'Mag u persoonsgegevens verwerken?' onder het kopje 'Vragen over grondslagen', 'Wanneer mag u zich baseren op de grondslag gerechtvaardigd belang?') Geraadpleegd op: 16 maart 2018

⁴⁰ Autoriteitpersoonsgegevens.nl (Zoek op: 'Mag u persoonsgegevens verwerken?' onder het kopje 'Vragen over grondslagen', 'Wanneer mag u zich baseren op de grondslag gerechtvaardigd belang?') Geraadpleegd op: 16 maart 2018

⁴¹ Autoriteitpersoonsgegevens.nl (Zoek op: 'Mag u persoonsgegevens verwerken?' onder het kopje 'Vragen over grondslagen', 'Wanneer mag u zich baseren op de grondslag gerechtvaardigd belang?') Geraadpleegd op: 16 maart 2018

⁴² Autoriteitpersoonsgegevens.nl (Zoek op: 'Mag u persoonsgegevens verwerken?' onder het kopje 'Vragen over grondslagen', 'Wanneer mag u zich baseren op de grondslag gerechtvaardigd belang?') Geraadpleegd op: 16 maart 2018

3.3 Zorgvuldigheid

De AVG dwingt organisaties om zorgvuldig om te gaan met persoonsgegevens van betrokkenen en hierover ook transparant te zijn naar de betrokkenen toe. Om deze zorgvuldigheid te kunnen waarborgen dient een organisatie bij de basis te beginnen en te zorgen dat het verwerken van persoonsgegevens op zich op een zorgvuldige wijze gebeurt. Ook hierbij geldt weer de verantwoordingsplicht. Op grond van de AVG is het voor een groot aantal organisaties dan ook verplicht om een Functionaris Gegevensbescherming in dienst te hebben. Daarnaast vraagt de AVG om Privacy by Design en Privacy by Default, en dient het VUmc Data Protection Impact Assessments uit te voeren. Voor een organisatie is het van belang om op zorgvuldige wijze persoonsgegevens te verwerken. Pas wanneer een organisatie dit intern op orde heeft kan zij naar de betrokkenen toe transparant zijn en aantonen dat zij op zorgvuldige wijze met persoonsgegevens omgaat.

Functionaris Gegevensbescherming

Met de invoering van de AVG wordt het op grond van artikel 37 AVG voor een groot aantal organisaties verplicht om een Functionaris Gegevensbescherming aan te stellen.⁴³ Het VUmc heeft inmiddels een Functionaris Gegevensbescherming aangesteld.

De positie van de Functionaris Gegevensbescherming ligt vastgelegd in artikel 38 van de AVG. De Functionaris Gegevensbescherming moet betrokken worden bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. Daarnaast moet hij toegang krijgen tot persoonsgegevens en verwerkingsactiviteiten, mag hij nooit ontslagen worden voor het uitvoeren van zijn taken en heeft hij een geheimhoudingsplicht.

De taken en verantwoordelijkheden van de Functionaris Gegevensbescherming worden in artikel 39 van de AVG nader beschreven. De Functionaris Gegevensbescherming dient:

- De verwerkingsverantwoordelijke of de verwerker en de werknemers die persoonsgegevens verwerken, te informeren en te adviseren over hun verplichtingen;
- toezicht te houden op de naleving van de AVG;
- desgevraagd advies te verstrekken met betrekking tot de gegevensbeschermingseffect-beoordeling en toezien op de uitvoering daarvan;
- met de Autoriteit Persoonsgegevens samen te werken;
- op te treden als contactpunt voor de Autoriteit Persoonsgegevens inzake met verwerking verband houdende aangelegenheden.

Privacy by Design and by Default

Artikel 25 van de AVG vraagt om Privacy by Design en Privacy by Default. In de Nederlandse versie van de AVG wordt dit vertaald als 'Gegevensbescherming door ontwerp en door standaardinstellingen'.

⁴³ Guidelines on Data Protection Officers ('DPOs'), 16/ EN, WP243, p.7, paragraaf 2.1.2

Privacy by Design houdt in dat organisaties al bij de ontwikkeling van producten en diensten privacyverhogende maatregelen dienen te nemen om te waarborgen dat het verwerken van persoonsgegevens op een zorgvuldige wijze plaatsvindt. Tevens dienen organisaties passende en organisatorische maatregelen te nemen om zich te houden aan minimale gegevensverwerking. Dit wordt Privacy by Default genoemd en houdt in dat organisaties in beginsel alléén persoonsgegevens mogen verwerken die noodzakelijk zijn voor het specifieke doel van de verwerking.⁴⁴ De technische en organisatorische maatregelen die hiervoor genomen moeten worden, worden besproken in paragraaf 3.4. Door middel van het nemen van voldoende maatregelen voldoet de organisatie aan het doelbindingsbeginsel en aan het beginsel van minimale gegevensverwerking.

Het is dus van belang dat een organisatie aan betrokkenen kan aantonen dat zij privacyverhogende maatregelen heeft genomen en dat zij alleen de gegevens verwerkt die noodzakelijk zijn voor het specifieke doel waarvoor de gegevens verwerkt worden.

Data Protection Impact Assessment

Wanneer een verwerking van persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, dient een organisatie op grond van artikel 35 AVG een Data Protection Impact Assessment (hierna: DPIA) uit te voeren. In het Nederlands wordt dit vertaald als Gegevensbeschermingseffect-beoordeling. Dit houdt in dat een organisatie bij risicovolle verwerkingen van persoonsgegevens de risico's en de impact van die verwerkingen in kaart moet brengen en vervolgens maatregelen moet nemen om die risico's te verkleinen.⁴⁵

In de gevallen waarin het voor een organisatie niet duidelijk is of een DPIA vereist is, omdat het niet duidelijk is of er sprake is van een hoog risico, raadt Werkgroep 29 aan om deze toch uit te voeren omdat een DPIA een nuttig instrument is dat verwerkingsverantwoordelijken helpt om aan de wetgeving inzake gegevensbescherming te voldoen.⁴⁶

Lid 2 van artikel 35 AVG verplicht de verwerkingsverantwoordelijke om bij de Functionaris Gegevensbescherming advies in te winnen over de uitvoering van de DPIA. Niet alleen het advies van de Functionaris Gegevensbescherming over de voorgenomen verwerking is van belang, maar ook de mening van de betrokkene. Betrokkenen moeten hier goed over geïnformeerd worden. Advocaat Ondernemingsrecht en Privacyrecht Marta Stephanian zegt hierover in een blog dat dit bijvoorbeeld kan middels een generieke studie, een vraag aan een ondernemingsraad of personeelsvertegenwoordiging, of door middel van enquêtes. Wanneer de verwerkingsverantwoordelijke besluit dat het niet passend is om de mening van de betrokkene te vragen, moet ook de motivering hiervoor gedocumenteerd worden.⁴⁷

⁴⁴ Autoriteitpersoonsgegevens.nl (Zoek op: 'Privacy by Design') Geraadpleegd op: 19 maart 2018

⁴⁵ Martha Stephanian, 'AVG Uitgediept #11: Wel of geen Data Protection Impact Assessment?' *tenholternoordam.nl* 5 december 2017

⁴⁶ Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 17/EN, WP 248 rev.01, p.8, paragraaf III

⁴⁷ Martha Stephanian, 'AVG Uitgediept #11: Wel of geen Data Protection Impact Assessment?' *tenholternoordam.nl* 5 december 2017

Het uitvoeren van DPIA's is dus van belang om uiteindelijk betrokkenen te kunnen verzekeren van een veilige verwerking van hun persoonsgegevens en hier ook in voldoende mate over te kunnen informeren.

3.4 Technische en organisatorische maatregelen

Een organisatie voldoet tevens aan de verantwoordingsplicht wanneer zij ingevolge artikel 24 lid 1 AVG voldoende technische en organisatorische maatregelen neemt om de privacy van betrokkenen te waarborgen. Op grond van de AVG moet een organisatie daarom ook een register van verwerkingsactiviteiten en een gegevensbeschermingsbeleid opstellen en de (digitale) beveiliging van de persoonsgegevens op orde hebben. Wanneer een organisatie deze verplichtingen op orde heeft kan zij de betrokkenen laten zien dat zij voldoet aan de regelgeving van de AVG.

Register van verwerkingsactiviteiten

Artikel 30 lid 1 in samenhang met lid 3 AVG stelt aan iedere organisatie meer dan 250 werknemers de verplichting om een register van verwerkingsactiviteiten op te stellen en bij te houden. Aangezien het VUmc meer dan 250 werknemers in dienst heeft, betekent dit voor haar dat zij een overzicht dient op te stellen en bij te houden van alle verwerkingen van persoonsgegevens die zij uitvoert. Iedere nieuwe verwerking die binnen het VUmc wordt uitgevoerd dient aan het register te worden toegevoegd. Deze verwerkingen kunnen een wettelijke grondslag hebben, maar dit kunnen ook verwerkingen zijn waarvoor toestemming gegeven is door de betrokkene.⁴⁸ Lid 2 van artikel 30 AVG bepaalt welke gegevens er in ieder geval moeten worden opgenomen in het register.

Het doel van het register van verwerkingsactiviteiten is om organisaties te dwingen concreet te worden over de persoonsgegevens die zij verzamelen, op welke wijze zij dat doen en met welk doel.⁴⁹ De Autoriteit Persoonsgegevens kan op verzoek inzage in het register vorderen om organisaties te controleren.⁵⁰ De informatie uit het register is dermate belangrijk dat zij de basis zal vormen voor het privacystatement dat organisaties aan betrokkenen dienen te verstrekken. Met een dergelijk register kan een organisatie betrokkenen namelijk grondiger informeren over de persoonsgegevens die zij verzameld, op welke manier en met doel. Op deze manier voldoet de organisatie dus weer aan haar transparantieplicht en aan haar verantwoordingsplicht.

Privacybeleid

Het opstellen van een gegevensbeschermingsbeleid, of te wel een privacybeleid, is een organisatorische maatregel die een organisatie moet nemen om te voldoen aan de transparantieplicht en de verantwoordingsplicht. De verplichting tot een privacybeleid is opgenomen in lid 2 van artikel 24 AVG. Aangezien dit gehele onderzoek is gericht op de

⁴⁸ Europadecentraal.nl (Zoek op: 'Register van verwerkingsactiviteiten') Geraadpleegd op: 20 maart 2018

⁴⁹ Engelfried, 'AVG compliance: het verwerkingsregister – vastleggen wat u doet met persoonsgegevens', *emerce.nl* 18 februari 2018

⁵⁰ Autoriteitpersoonsgegevens.nl (Zoek op: 'Verantwoordingsplicht') Geraadpleegd op: 20 maart 2018

inrichting van het privacybeleid van het VUmc, zal op dit onderwerp in hoofdstuk 4 uitgebreid worden ingegaan.

(Digitale) beveiliging

Artikel 32 AVG verplicht organisaties om hun beveiligingsniveau af te stemmen op de risico's die de verwerking van gegevens met zich meebrengt. Risico's die in dit artikel bedoeld worden zijn vernietiging, verlies, wijziging of ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens. Om deze risico's in te perken moeten er op grond van artikel 31 lid 1 AVG maatregelen overwogen worden die nodig zijn voor:

- De pseudonimisering en versleuteling van persoonsgegevens;
- het op permanente basis garanderen van de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten;
- het tijdig herstellen van de beschikbaarheid van en de toegang tot de persoonsgegevens bij een fysiek of technisch incident;
- een procedure om op gezette tijdstippen de doeltreffendheid van de technische en organisatorische maatregelen te testen, te beoordelen en te evalueren, ter beveiliging van de verwerking.

De beveiligingsmaatregelen die worden getroffen moeten op grond van artikel 30 lid 1 sub g AVG worden opgenomen in het register van verwerkingsactiviteiten. Daarnaast vermeldt artikel 35 lid 9 AVG dat bij een DPIA aandacht dient te worden besteed aan de beveiliging van de verwerkingen.

Door middel van het goed beveiligen van de verwerkingen van persoonsgegevens nemen organisaties hun verantwoordingsplicht serieus. Daarnaast is het wegens de transparantieplicht van belang dat organisaties betrokkenen kunnen verzekeren van een goede beveiliging van de verwerking van hun gegevens.

3.5 Rechten van betrokkenen

De AVG kent verscheidene rechten toe aan personen van wie persoonsgegevens worden verwerkt. Dit worden 'betrokkenen' genoemd. Een aantal van deze rechten liggen ook al vastgelegd in de Wbp. De AVG is echter, zoals eerder genoemd, gericht op transparantie. Betrokkenen hebben hierdoor dus meer rechten gekregen om te controleren hoe er met hun gegevens wordt omgegaan.

Recht op informatie

Het recht op informatie ligt vastgelegd in artikel 13 en 14 van de AVG. Wanneer er persoonsgegevens van een betrokkene worden verwerkt moet hij hiervan door de organisatie op de hoogte worden gesteld. Daarnaast moet de betrokkene op grond van de genoemde artikelen onder meer geïnformeerd worden over de specifieke doeleinden waarvoor de gegevens worden verwerkt, wat de gerechtvaardigde belangen zijn, de periode waarin de

gegevens worden gebruikt, dat de betrokkene recht heeft op inzage en dat hij een klacht kan indienen bij de Autoriteit Persoonsgegevens. Het recht op informatie voor de betrokkene is een informatieplicht voor de organisatie en is dan ook de grondslag voor het opstellen van een extern privacybeleid en een privacystatement. In dit onderzoek zal dan ook met name de nadruk liggen op de informatieplicht.

Recht van inzage

Zoals zojuist benoemd heeft de betrokkene ook recht op inzage. Dit recht ligt vastgelegd in artikel 15 van de AVG. De betrokkene heeft recht om inzage te krijgen in welke persoonsgegevens er verwerkt worden maar heeft onder meer ook recht om inzage te krijgen in de informatie over de verwerkingsdoeleinden en aan welke ontvangers deze persoonsgegevens worden verstrekt. Daarnaast zijn organisaties verplicht om een kopie van de te verwerken persoonsgegevens aan de betrokkene te verschaffen.

Recht op rectificatie

Artikel 16 van de AVG geeft betrokkenen het recht om van de verwerkingsverantwoordelijke onverwijld rectificatie van de hem betreffende onjuiste persoonsgegevens te verkrijgen. De betrokkene heeft het recht om vervollediging van onvolledige persoonsgegevens te verkrijgen. Betrokkene kan deze onvolledige gegevens aanvullen door onder meer een aanvullende verklaring te verstrekken aan de organisatie.

Recht op gegevenswissing

Het recht op gegevenswissing wordt ook wel het recht op vergetelheid genoemd en is een nieuw recht onder de AVG. Dit recht ligt vastgelegd in artikel 17 van de AVG. Dit artikel geeft betrokkenen het recht om onder bepaalde voorwaarden de verwerkingsverantwoordelijke wissing van de hem betreffende persoonsgegevens te verzoeken.

In tegenstelling tot de andere rechten is artikel 17 op grond van lid 2 van dit artikel echter niet van toepassing op de verwerking van persoonsgegevens in de gezondheidszorg en geldt dit recht dus ook niet voor patiënten van het VUmc.

Recht op beperking van de verwerking

Het recht op beperking van de verwerking is een nieuw recht onder de AVG en ligt vastgelegd in artikel 18 van de AVG. Dit recht houdt in dat betrokkenen in bepaalde situaties recht hebben de verwerking van hun persoonsgegevens (tijdelijk) te stoppen.⁵¹ Wanneer een betrokkene dit recht inzet mag de organisatie de gegevens dus niet meer wijzigen of verwerken, totdat de betrokkene weer toestemming geeft.

Recht op overdraagbaarheid

Het recht op overdraagbaarheid wordt ook wel het recht op dataportibiliteit genoemd en is een nieuw recht onder de AVG. Het recht op overdraagbaarheid is vastgelegd in artikel 20 van de AVG en houdt in dat een betrokkene onder bepaalde voorwaarden het recht heeft de

⁵¹ Arts, 'Hoe geef je invulling aan de verschillende rechten van betrokkenen: het recht op beperking van de verwerking', *Privacycompany.eu* 5 september 2017

persoonsgegevens die hij aan een organisatie heeft verstrekt, in een gestructureerde, gangbare en machineleesbare vorm te verkrijgen. Daarnaast heeft de betrokkene het recht die gegevens aan een andere verwerkingsverantwoordelijke over te dragen, zonder daarbij te worden gehinderd door de organisatie. Ook kan de betrokkene, indien dit technisch mogelijk is, eisen dat de organisatie de persoonsgegevens rechtsreeks overdraagt aan een andere verwerkingsverantwoordelijke.

Recht van bezwaar

Het recht van bezwaar houdt in dat een betrokkene bezwaar mag maken tegen de verwerking van zijn persoonsgegevens wanneer dit verband houdt met zijn specifieke situatie. Dit is alleen toegestaan wanneer de persoonsgegevens worden verwerkt op basis van gerechtvaardigd belang of algemeen belang.⁵² Hiervoor moet er wel voldaan worden aan de voorwaarden die genoemd staan in artikel 21 AVG. Wanneer een betrokkene dit recht inroept is de organisatie verplicht de verwerking van de persoonsgegevens te staken, tenzij zij dwingende gerechtvaardigde gronden voor de verwerking aanvoert.

Recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming, waaronder profiling

Dit recht is al vastgelegd in de Wbp maar wordt in de AVG in artikel 22 nieuw leven ingeblazen. Op grond van dit artikel heeft een betrokkene dan ook het recht om niet te worden onderworpen aan geautomatiseerde besluitvorming, zonder menselijke tussenkomst, wanneer er rechtsgevolgen zijn verbonden aan zo een geautomatiseerd besluit of wanneer het de betrokkene in aanmerkelijke mate treft.⁵³ Op een aantal uitzonderingen na moet er voor het kunnen verwerken van persoonsgegevens dus eerst menselijk contact zijn geweest.

3.6 Toezicht

Zoals eerder genoemd wordt er in de AVG meer nadruk gelegd op de verantwoordingsplicht van organisaties. Organisaties moeten kunnen aantonen dat zij aan de AVG voldoen. Dit wordt ook wel accountability genoemd. Daarnaast zijn organisaties onder meer verplicht zich te houden aan het transparantiebeginsel.

Omdat het digitaal verwerken van persoonsgegevens toeneemt, is het voor organisaties van groot belang dat zij hun verantwoordelijkheid nemen en passende maatregelen treffen om persoonsgegevens te beveiligen en af te schermen voor onbevoegden. Daarnaast is het van belang dat zij over het proces van gegevensbescherming ook transparant zijn naar de betrokkenen toe.

⁵² Arts, 'Hoe geef je invulling aan de verschillende rechten van betrokkenen: het recht van bezwaar', *Privacycompany.eu* 14 augustus 2017.

⁵³ Visser, 'Hoe geef je invulling aan de verschillende rechten van betrokkenen: geautomatiseerde besluiten en profiling', *Privacycompany.eu* 7 augustus 2017.

Wanneer een organisatie de AVG overtreedt kan er door de Autoriteit Persoonsgegevens een boete worden opgelegd. Er worden twee soorten boetes onderscheiden:

1. Komt de organisatie een van zijn verplichtingen, zoals de verantwoordingsplicht, niet na? Dan kan de Autoriteit Persoonsgegevens een boete opleggen van maximaal 10 miljoen euro of een boete van 2% van de wereldwijde jaaromzet, mocht dat bedrag hoger uitkomen.
2. Overtreedt de organisatie de beginselen of grondslagen van de AVG? Of de privacyrechten van de betrokkenen? Dan kan de AP een boete opleggen van maximaal 20 miljoen euro of een boete van 4% van de wereldwijde jaaromzet, mocht dat bedrag hoger uitkomen.⁵⁴

Door middel van het opstellen van een juist extern privacybeleid voldoet een organisatie in ieder geval aan het transparantieprincipe en kan zij hiermee een boete voorkomen.

⁵⁴ Autoriteitpersoonsgegevens.nl (Zoek op: 'Algemene informatie AVG') Geraadpleegd op: 26 maart 2018

Hoofdstuk 4: Het extern privacybeleid

In dit hoofdstuk wordt specifiek ingegaan op de wet- en regelgeving rondom de inrichting en uitvoering van het extern privacybeleid van organisaties. Allereerst wordt de grondslag voor het opstellen van een privacybeleid besproken. Vervolgens wordt er gekeken naar wat een dergelijk beleid precies inhoudt. Daarna worden de vanuit de wet gestelde eisen aan het privacybeleid, de inhoud en de vormgeving hiervan besproken. Tot slot wordt er ingegaan op de communicatiekanalen waarop het extern privacybeleid zou moeten worden verspreid en de momenten waarop organisaties het extern privacybeleid onder de aandacht van betrokkenen moeten brengen.

4.1 Grondslag privacybeleid

Artikel 12 AVG verplicht organisaties passende maatregelen te nemen om betrokkenen te informeren over privacy. Deze verplichting wordt ook wel de transparantieplicht genoemd en houdt verband met de verantwoordingsplicht uit artikel 24 AVG, welke wij eerder bespreken. Organisaties dienen namelijk niet alleen aan de Autoriteit Persoonsgegevens verantwoording af te leggen over de wijze waarop zij met privacy omgaan, maar ook aan de betrokkenen. Organisaties moeten kunnen aantonen dat zij voldoen aan de wetgeving van de AVG en dat zij zorgvuldig met gegevens van betrokkenen omgaan.

4.2 Tweeledig beleid

De maatregelen die genomen dienen te worden om aan de transparantieplicht en de verantwoordingsplicht te voldoen, omvatten ingevolge artikel 24 lid 2 AVG het opstellen en uitvoeren van een gegevensbeschermingsbeleid. In de praktijk wordt het gegevensbeschermingsbeleid ook wel 'privacybeleid' genoemd.⁵⁵ Een privacybeleid is tweeledig. In eerste instantie dient iedere organisatie een intern privacybeleid te hebben. Dit beleid is om aan te kunnen tonen dat de verwerking van persoonsgegevens in overeenstemming is met de AVG. Een intern privacybeleid wordt binnen de organisatie zelf gebruikt en geldt voor alle medewerkers die te maken krijgen met het verwerken van persoonsgegevens en andere privacygevoelige informatie.⁵⁶ Bij het opstellen van een dergelijk nieuw beleid dienen de beginselen van Privacy by design and by default te worden betrokken.⁵⁷

Een intern privacybeleid is ingevolge artikel 24 lid 1 AVG dus bedoeld om te waarborgen en te kunnen aantonen dat de verwerking van persoonsgegevens in overeenstemming met de AVG wordt uitgevoerd. Organisaties dienen op grond van artikel 12 AVG dit echter ook aan te

⁵⁵ Aangezien in de praktijk wordt gesproken over 'privacybeleid' zal in dit onderzoek ook deze term worden gehanteerd.

⁵⁶ Van der Zwan, 'PRIVACYBELEID: wat staat daar in?', *Linkedin.com* 12 september 2016 <https://nl.linkedin.com/pulse/privacybeleid-wat-staat-daar-kirsten-van-der-zwan>

⁵⁷ Kamerstukken II 2017/18, 34851, 3, p. 45 (MvT)

kunnen tonen en uit te kunnen leggen aan betrokkenen. Een intern privacybeleid mag echter niet worden gebruikt om aan betrokkenen bekend te maken. Hiervoor moet een extern privacybeleid worden opgesteld.⁵⁸

4.3 Eisen extern privacybeleid

Het informeren van betrokkenen over de verwerking van hun persoonsgegevens was in artikel 33 en 34 van de Wbp ook al verplicht was gesteld. In deze artikelen ligt echter slechts vastgelegd *dat* betrokkenen moeten worden geïnformeerd en ligt niet vastgelegd op *welke wijze* dat dient te gebeuren. Veel organisaties hebben daarom geen idee hoe ze hier invulling aan moeten geven en hebben daarom hun intern privacybeleid op de website geplaatst.⁵⁹ Dit zijn vaak erg langdradige en technisch of juridisch complexe stukken die betrokkenen niet begrijpen. Andere organisaties hebben in het geheel geen privacybeleid op hun website geplaatst.

Om aan deze onduidelijkheid een einde te maken heeft de AVG wel specifieke eisen gesteld aan de wijze waarop informatie over het verwerken van persoonsgegevens verstrekt dient te worden. Artikel 12 lid 1 AVG stelt namelijk de eis dat deze informatie op een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal verstrekt dient te worden. In artikel 12 AVG wordt daarnaast benadrukt dat deze informatie ook voor kinderen begrijpelijk dient te zijn. Considerans sub 58 van de AVG vult hierop aan dat wanneer de verwerking specifiek tot een kind is gericht, de informatie en communicatie in een zodanig duidelijke en eenvoudige taal dient te worden gesteld dat het kind deze makkelijk kan begrijpen.

De wetgever heeft het dus noodzakelijk geacht dat betrokkenen ook daadwerkelijk begrijpen wat er in een dergelijk extern privacybeleid staat. Betrokkenen moeten dus zonder veel moeite kunnen begrijpen welke persoonsgegevens van hen worden gevraagd, voor welke doeleinden deze worden gebruikt en wat hun rechten zijn. De AVG stelt dus zwaardere eisen aan een extern privacybeleid dan de Wbp deed.

4.4 Inhoud extern privacybeleid

Naast dat de AVG eisen stelt aan de begrijpelijkheid van het extern privacybeleid, stelt de AVG in artikel 13 ook eisen aan welke informatie er verstrekt dient te worden. Organisaties dienen op grond van dit artikel bij verkrijging van de persoonsgegevens al de volgende informatie aan betrokkenen te verschaffen:

1. De identiteit en de contactgegevens van de verantwoordelijke;
2. de contactgegevens van de Functionaris Gegevensbescherming;
3. de doeleinden en de rechtsgrond van de verwerking van de persoonsgegevens;

⁵⁸ Van der Zwan, 'PRIVACYBELEID: wat staat daar in?', *Linkedin.com* 12 september 2016 <https://nl.linkedin.com/pulse/privacybeleid-wat-staat-daar-kirsten-van-der-zwan>

⁵⁹ Van der Zwan, 'PRIVACYBELEID: wat staat daar in?', *Linkedin.com* 12 september 2016 <https://nl.linkedin.com/pulse/privacybeleid-wat-staat-daar-kirsten-van-der-zwan>

4. de gerechtvaardigde belangen van de verwerkingsverantwoordelijke, indien de verwerking op het gerechtvaardigd belang is gebaseerd;
5. de ontvangers of categorieën van ontvangers van de persoonsgegevens;
6. of de persoonsgegevens (zullen) worden doorgestuurd aan een derde land buiten de EU.

Naast deze informatie dienen organisaties ook de volgende aanvullende informatie te verschaffen om een behoorlijke en transparante verwerking te waarborgen:

7. De bewaartermijn van de persoonsgegevens, of indien dat niet mogelijk is, de criteria ter bepaling van het bewaartermijn;
8. welke rechten de betrokkene heeft;
9. dat de betrokkene het recht heeft de toestemming te allen tijde in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de verwerking;
10. dat de betrokkene het recht heeft een klacht in te dienen bij de toezichthouder;
11. of de verstrekking van persoonsgegevens een wettelijke of contractuele verplichting is dan wel een noodzakelijke voorwaarde om een overeenkomst te sluiten, en of de betrokkene verplicht is de persoonsgegevens te verstrekken en wat de mogelijke gevolgen zijn wanneer deze gegevens niet worden verstrekt;
12. of de organisatie gebruik maakt van geautomatiseerde besluitvorming, de reden waarom zij dit doet, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

Wanneer organisaties de gegevens niet van de betrokkene zelf hebben ontvangen, dienen zij ingevolge artikel 14 AVG de betrokkenen ook te informeren over de bron waar de persoonsgegevens vandaan komen.

Werkgroep 29 heeft in een van haar richtlijnen een nadere aanvulling gegeven op deze artikelen. In *Guidelines on transparency under Regulation* geeft zij aan dat het transparantiebeginsel niet alleen inhoudt dat organisaties de voorgeschreven informatie uit artikel 13 en 14 dienen te verstrekken, maar dat dit beginsel ook inhoudt dat de betrokkene vooraf moet kunnen bepalen wat de reikwijdte en de gevolgen van de verwerking met zich meebrengt. Volgens de werkgroep dienen organisaties daarom ook afzonderlijk in ondubbelzinnige taal te beschrijven wat de belangrijkste gevolgen van de verwerking zal zijn. Er moet dus duidelijk worden weergegeven wat voor effect de specifieke verwerking die wordt beschreven in een privacystatement feitelijk heeft op een betrokkene. Deze beschrijving van de gevolgen van de verwerking mag niet berusten op onschuldige en voorspelbare 'best case' voorbeelden van gegevensverwerking, maar moet een overzicht bieden van de soorten verwerking die de grootste impact kunnen hebben op de fundamentele rechten en vrijheden

van gegevens van betrokkenen met betrekking tot de bescherming van hun persoonlijke gegevens.⁶⁰

4.5 Vormgeving extern privacybeleid

Zoals hiervoor besproken stelt artikel 12 lid 1 AVG de eis dat organisaties 'passende maatregelen' dienen te nemen om informatie aan betrokkenen in ieder geval op een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal te verstrekken. De AVG zegt echter niets over de vorm waarop deze informatie verstrekt dient te worden, er wordt slechts voorgeschreven dat dit schriftelijk dient te gebeuren.

Werkgroep 29 geeft in *Guidelines on transparency under Regulation* aan dat de vorm en de manier waarop de krachtens artikel 13 en 14 vereiste informatie aan betrokkenen moet worden verstrekt van groot belang is. In deze richtlijn geeft zij dan ook advies over de wijze waarop het extern privacybeleid kan worden ingericht. Om zich te kunnen houden aan het vereiste dat de informatievoorziening aan en de communicatie met betrokkenen op een 'beknopte en transparante' manier plaatsvindt, dienen organisaties de informatie en communicatie op efficiënte en beknopte wijze te presenteren. Hierbij is het volgens de werkgroep van belang om de informatie te scheiden van andere niet- privacygerelateerde informatie.⁶¹ Werkgroep 29 geeft organisaties het advies om bij het bepalen van de vorm van de informatieverstrekking rekening te houden met alle omstandigheden van de gegevensverzameling- en verwerking. Hierbij moet er bijvoorbeeld worden gekeken naar de 'reis' die betrokkenen maken op de website.⁶² Op deze wijze kan er goed worden ingespeeld op de informatie die betrokkenen wensen te lezen. Werkgroep 29 geeft organisaties dan ook het advies om op hun website⁶³ een gelaagd privacystatement op te stellen.⁶⁴ Hierdoor stelt men betrokkenen in staat om naar dat specifieke gedeelte van het statement te gaan waar zij in geïnteresseerd zijn en voorkomt men dat betrokkenen grote hoeveelheden tekst moeten doorzoeken waardoor zij het overzicht verliezen.⁶⁵

Om aan de schriftelijkheidseis van artikel 12 AVG te voldoen, adviseert Werkgroep 29 organisaties dus om een gelaagd privacystatement op hun website op te stellen. Naast dat de informatieverstrekking op grond van de AVG schriftelijk dient te zijn, staat de AVG volgens Werkgroep 29 ook andere, niet-gespecificeerde 'middelen' zoals elektronische middelen toe. Artikel 12 lid 7 AVG en, in aanvulling daarop, considerans sub 58 en sub 60 van de AVG geven namelijk aan dat er bij het verstrekken van de informatie aanvullende visualisatie gebruikt moet worden om de informatie nog meer de verduidelijken. Daarnaast mogen er ter onderbouwing van deze informatie gestandaardiseerde icoontjes gebruikt worden. Naast het

⁶⁰ Guidelines on transparency under Regulation 2016/679, 17/ EN, WP260, p. 8, paragraaf 9

⁶¹ Guidelines on transparency under Regulation 2016/679, 17/ EN, WP260, p. 7, paragraaf 7

⁶² Guidelines on transparency under Regulation 2016/679, 17/ EN, WP260, p. 13, paragraaf 20

⁶³ Guidelines on transparency under Regulation 2016/679, 17/ EN, WP260, p. 13, paragraaf 20

⁶⁴ Guidelines on transparency under Regulation 2016/679, 17/ EN, WP260, p. 7, paragraaf 7

⁶⁵ Guidelines on transparency under Regulation 2016/679, 17/ EN, WP260, p. 10, paragraaf 14

gebruik van deze icoontjes mogen er volgens de werkgroep ter aanvulling van het privacystatement ook andere elektronische middelen worden gebruikt. Hierbij kan gedacht worden aan pop-upberichten, 3D-touch of hover-over notices, privacy-dashboards, video's en smartphones of IoT-voice alerts. Andere mogelijkheden om het privacystatement aan te vullen of te onderbouwen zijn volgens Werkgroep 29 het gebruik van cartoons, infographics of stroomdiagrammen.⁶⁶

Naast het advies om aanvullende elektronische middelen te gebruiken, stelt Werkgroep 29 ook een aantal eisen aan het gelaagde privacystatement. Het ontwerp en de lay-out van de eerste laag van het statement moeten volgens de werkgroep zodanig ingericht zijn dat de betrokkene een duidelijk overzicht heeft van de informatie over de verwerking van zijn persoonsgegevens. Daarnaast moet duidelijk zijn waar betrokkenen kunnen doorklikken naar een onderstaande laag om meer gedetailleerde informatie te kunnen lezen. Tevens is het van belang dat de informatie in de verscheidene lagen consistent is en dat de lagen geen tegenstrijdige informatie bevatten. Met betrekking tot de inhoudelijke informatie die in de eerste laag van het privacystatement kan worden opgenomen, is het standpunt van Werkgroep 29 dat dit altijd informatie moet bevatten over de verwerking die de grootste impact heeft op de betrokkene. Daarom moet de betrokkene uit de informatie in de eerste laag kunnen begrijpen wat de gevolgen van de verwerking van zijn persoonsgegevens zijn.⁶⁷

4.6 Communicatiekanalen extern privacybeleid

Artikel 12 AVG schrijft voor dat de informatie over gegevensverwerking in een gemakkelijk toegankelijke vorm verstrekt dient te worden. Volgens Werkgroep 29 betekent 'gemakkelijk toegankelijk' dat de betrokkenen de informatie niet op hoeven te zoeken, maar dat het voor hen direct duidelijk is waar zij deze informatie kunnen vinden.⁶⁸

Het extern privacybeleid kan via verscheidene wegen en middelen worden gecommuniceerd naar betrokkenen. Werkgroep 29 geeft organisaties allereerst het advies om op hun website een link te hebben naar het privacystatement. *Deze link moet duidelijk opvallend en duidelijk zijn zichtbaar zijn onder een veelgebruikte term als 'Privacy', 'Privacybeleid' of 'Kennisgeving inzake gegevensbescherming'.*⁶⁹

Ook voor informatieverstrekking via apps heeft Werkgroep 29 richtlijnen opgesteld. Zo moet de *benodigde informatie voorafgaand aan het downloaden ook beschikbaar zijn via de online store waarin de app te downloaden is. Nadat de app geïnstalleerd is mag de informatie nooit meer dan "twee tikken verwijderd" zijn. Dit houdt in de praktijk in dat de menufunctie van de app altijd een optie 'Privacy' of 'Gegevensbescherming' moet bevatten.*⁷⁰

⁶⁶ Guidelines on transparency under Regulation 2016/679, 17/ EN, WP260, p. 10-11, paragraaf 14

⁶⁷ Guidelines on transparency under Regulation 2016/679, 17/ EN, WP260, p. 17, paragraaf 30

⁶⁸ Guidelines on transparency under Regulation 2016/679, 17/ EN, WP260, p. 8, paragraaf 10

⁶⁹ Guidelines on transparency under Regulation 2016/679, 17/ EN, WP260, p. 8, paragraaf 10

⁷⁰ Guidelines on transparency under Regulation 2016/679, 17/ EN, WP260, p. 8, paragraaf 10

Hoewel de voorkeur van Werkgroep 29 uitgaat naar online verstrekking van informatie via een privacystatement, moeten er volgens de werkgroep ook mogelijkheden zijn om het beleid via andere wegen te verstrekken. Een van de mogelijkheden is het hard copy verstrekken van informatie. Dit kan bijvoorbeeld door middel van schriftelijke toelichtingen, folders, informatie in contractuele documenten, maar ook door middel van de al reeds genoemde cartoons, infographics of stroomdiagrammen.⁷¹ Organisaties kunnen er ook voor kiezen om de link van het online privacystatement op te nemen in papieren handleidingen en folders of het gehele privacystatement op te nemen in deze handleidingen en folders.⁷²

Een andere optie is om betrokkenen mondeling te informeren. Dit kan via persoonlijk contact of telefonisch. Hierbij kunnen betrokkenen mondelinge uitleg van een medewerker krijgen of door middel van geautomatiseerde of vooraf opgenomen informatie worden geïnformeerd. Ook kan er gebruik worden gemaakt van screenless smart technologie zoals pictogrammen, QR-codes, gesproken of geschreven instructies, video's, SMS-of e-mailberichten, narrow casing, of voorlichtingscampagnes.⁷³

4.7 Momenten van informatieverstrekking

Zoals we bespraken kunnen organisaties door middel van het opstellen van een privacybeleid voldoen aan het transparantiebeginsel. Werkgroep 29 geeft in haar transparantierichtlijn aan dat het transparantievereiste echter niet slechts op het moment van verzameling van persoonsgegevens geldt, maar gedurende de gehele cyclus van de verwerking. Organisaties dienen betrokkenen dus te informeren wanneer een wijziging optreedt in bijvoorbeeld de inhoud of de voorwaarden van het privacybeleid.⁷⁴ Werkgroep 29 wijst organisaties er op dat *indien de wijziging van de informatie wijst op een fundamentele wijziging in de aard van de verwerking (bijvoorbeeld de uitbreiding van de categorieën ontvangers of de invoering van overdrachten naar een derde land) of een wijziging die misschien niet fundamenteel is voor de verwerking, maar die van belang kan zijn en gevolgen kan hebben voor de betrokkene, die informatie ruim vóór de daadwerkelijke inwerkingtreding van de wijziging aan de betrokkene dient te worden verstrekt. De methode die wordt gebruikt om de wijzigingen onder de aandacht van de betrokkene te brengen dient expliciet en doeltreffend te zijn.*⁷⁵ Hierbij dienen organisaties dus alle nodige maatregelen te nemen om ervoor te zorgen dat deze wijzigingen ook daadwerkelijk worden opgemerkt bij de betrokkenen. De wijze waarop dit wordt gecommuniceerd dient daarom ook volledig gewijd te zijn aan de wijzigingen en mag geen andere onderwerpen bevatten.⁷⁶

Ook wanneer informatie over gegevensverwerking, zoals het privacystatement, niet wezenlijk verandert is het volgens Werkgroep 29 van belang om betrokkenen te blijven informeren over deze zaken. Betrokkenen zullen namelijk na een tijd de aan hen verstrekte informatie niet

⁷¹ Guidelines on transparency under Regulation 2016/679, 17/ EN, WP260, p. 18-19, paragraaf 33

⁷² Guidelines on transparency under Regulation 2016/679, 17/ EN, WP260, p. 11, paragraaf 15

⁷³ Guidelines on transparency under Regulation 2016/679, 17/ EN, WP260, p. 18-19, paragraaf 33

⁷⁴ Guidelines on transparency under Regulation 2016/679, 17/ EN, WP260, p. 13, paragraaf 22

⁷⁵ Guidelines on transparency under Regulation 2016/679, 17/ EN, WP260, p. 15-16, paragraaf 26

⁷⁶ Guidelines on transparency under Regulation 2016/679, 17/ EN, WP260, p. 13, paragraaf 22

meer herinneren. Voor die situaties, waarbij de gegevensverwerking doorlopend plaatsvindt, dienen organisaties de betrokkenen opnieuw op de hoogte stellen van de reikwijdte van de gegevensverwerking. Dit kan bijvoorbeeld middels een periodieke herinnering aan het privacystatement.⁷⁷

⁷⁷ Guidelines on transparency under Regulation 2016/679, 17/ EN, WP260, p. 16, paragraaf 28

Hoofdstuk 5: Het extern privacybeleid in de praktijk

Na het uitvoeren van het theoretisch onderzoek, wat uitgewerkt is in de vorige hoofdstukken, is er nog een aantal zaken niet duidelijk geworden uit literatuur en wetgeving. Hierbij gaat het voornamelijk om de vraag hoe de wetgeving met betrekking tot het extern privacybeleid vertaald moet worden naar de praktijk van het VUmc. Om deze reden is er praktijkonderzoek uitgevoerd door middel van het afnemen van interviews met een aantal medewerkers van het VUmc en het AMC.⁷⁸

Alle personen waarmee een interview is afgenomen zijn direct of indirect betrokken bij het opstellen en uitvoeren van het extern privacybeleid. De transcripties van deze interviews zijn opgenomen onder Bijlage V. Aangezien de medewerkers op verscheidene vakgebieden deskundig zijn, zijn de interviewvragen deels aangepast aan het vakgebied en de deskundigheid van de betreffende medewerker.

De interviewvragen zijn gebaseerd op deelvragen 4, 5, 6 en 7 en daarom onderverdeeld in de volgende topics: 'Algemeen', 'Het extern privacybeleid onder de Wbp en onder de AVG', 'Communicatiekanalen van het extern privacybeleid' en 'De uitvoering van het extern privacybeleid'. Deze topics zullen in dit hoofdstuk aan bod komen.

Tevens is er aan de participanten een aantal vragen gesteld wat wel opgenomen is in de bijlage, maar niet terugkomt in de resultaten. Er is voor gekozen om deze vragen niet in de resultaten terug te laten komen omdat deze vragen niet relevant zijn voor het beantwoorden van de centrale vraag, maar wel relevant zijn voor voldoende achtergrondinformatie van de situatie binnen het VUmc.

Bij topic 1 'Algemeen' zijn er aan de participanten vragen voorgelegd met betrekking tot de verwerking van persoonsgegevens binnen het VUmc en het belang van een gedegen extern privacybeleid. Deze vragen zijn allereerst gesteld om een algemeen beeld te krijgen van de wijze waarop er persoonsgegevens worden verzameld bij het VUmc, ten tweede om te onderzoeken welke informatie met betrekking tot persoonsgegevens in het nieuwe extern privacybeleid vermeldt moeten worden, en ten derde om vanuit verscheidene invalshoeken het belang en de waarde van een gedegen extern privacybeleid binnen het VUmc vast te stellen. De interviewresultaten bij deze topic worden besproken in paragraaf 5.1.

Bij topic 2 'Huidig en toekomstig extern privacybeleid' zijn er aan de participanten vragen voorgelegd met betrekking tot de inrichting en uitvoering van het huidige en het toekomstige extern privacybeleid. Deze methode is gebruikt om een beeld te krijgen van het huidige extern privacybeleid van het VUmc en de tekortkomingen die er nog zijn met betrekking tot

⁷⁸ Hoewel het onderzoek in opdracht van het VUmc wordt uitgevoerd zullen het VUmc en het AMC op termijn eenzelfde extern privacybeleid gaan hanteren. Om deze reden is het van belang om ook de mening van medewerkers van het AMC mee te nemen in het onderzoek.

het extern privacybeleid onder de AVG. De interviewresultaten bij deze topic worden besproken in paragraaf 5.2.

Bij Topic 3 'Communicatiekanalen extern privacybeleid' zijn er aan de participanten vragen voorgelegd met betrekking tot de kanalen waarover het toekomstige extern privacybeleid gecommuniceerd moet worden naar de patiënten. Hierbij is er specifiek doorgevraagd naar de invulling van het privacystatement en het gebruik van een folder. Deze vragen zijn gesteld omdat Werkgroep 29 nadruk legt op de wijze van communiceren, en dan met name op het privacystatement en een folder. De interviewresultaten bij deze topic worden besproken in paragraaf 5.3.

Bij de topic 4 'Uitvoering en toezicht extern privacybeleid' zijn er aan de participanten vragen voorgelegd met betrekking tot de uitvoering van het toekomstige extern privacybeleid en de toezicht hierop. Deze vragen zijn gesteld omdat het voor het VUmc niet alleen van belang is dat zij een gedegen extern privacybeleid opstelt, maar het ook van belang is dat de medewerkers van het VUmc het beleid goed uitvoeren en hier toezicht op gehouden wordt, om zo aan de verantwoordingsplicht te blijven voldoen. De interviewresultaten bij deze topic worden besproken in paragraaf 5.4.

5.1 Algemeen

5.1.1 Persoonsgegevens

Uit voorgaande hoofdstukken blijkt dat de AVG in artikel 13 organisaties verplicht om in hun extern privacybeleid op te nemen welke persoonsgegevens zij verwerken. Om dit op te kunnen nemen in het extern privacybeleid en transparant te zijn tegenover haar patiënten, is het voor het VUmc allereerst van belang om helder te hebben welke persoonsgegevens zij precies verwerkt, op welke wijzen zij deze gegevens verzameld en voor welke doeleinden deze gegevens verzameld worden.

Soorten persoonsgegevens

Een ziekenhuis verwerkt veel soorten persoonsgegevens. Hierbij wordt een onderscheid gemaakt tussen gewone en bijzondere persoonsgegevens.⁷⁹ Uit de afgenomen interviews blijkt dat binnen het ziekenhuis onder de gewone persoonsgegevens voornamelijk de NAW-gegevens van de patiënt⁸⁰, het Burgerservicenummer van de patiënt, de naam van de verzekeraar, de vorm van de verzekering en eventueel gegevens van contactpersonen zoals familie of begeleiders vallen.⁸¹ Dit worden ook wel de administratieve persoonsgegevens genoemd en zijn nodig om te weten wie de patiënt is, maar ook om de factuur te kunnen sturen.⁸²

De bijzondere gegevens die van patiënten worden verzameld kunnen zijn: Religie, seksuele

⁷⁹ Zie interview 1, bijlage V, p. 54

⁸⁰ Zie interview 1, bijlage V, p. 54, interview 2, bijlage V, p. 64, interview 3, bijlage V, p. 72, interview 5, bijlage V, p. 88, interview 9, bijlage V, p. 117

⁸¹ Zie interview 5, bijlage V, p. 88-89, interview 9, bijlage V, p. 117

⁸² Zie interview 9, bijlage V, p. 117

geaardheid, godsdienst en lidmaatschap van een vakbond. Onder bijzondere persoonsgegevens vallen ook de diagnose, de nevendiagnose en medicatie.⁸³ Dit worden ook wel medische gegevens genoemd en zijn hoog privacygevoelige persoonsgegevens.⁸⁴ Medische gegevens zijn nodig voor de dossiervoering en om zorg te kunnen leveren. Vanuit de WGBO is het ook verplicht om deze gegevens vast te leggen.⁸⁵

Hoewel in de wet dus wordt gesproken over gewone en bijzondere persoonsgegevens, is de Functionaris Gegevensbescherming van het VUmc van mening dat dit in een ziekenhuis wat breder moet worden gezien. Volgens hem is er sprake van een opbouw van vier soorten persoonsgegevens namelijk: Gewone persoonsgegevens, sensitieve persoonsgegevens, bijzondere persoonsgegevens en heel bijzondere persoonsgegevens. Onder gewoon en bijzonder vallen dan de gegevens die we zojuist bespraken. Sensitief is volgens de Functionaris Gegevensbescherming bijvoorbeeld dat een patiënt een afspraak heeft bij de cardiologie. Men kan aan die afspraak al zien dat de patiënt iets aan zijn hart heeft. Onder heel bijzonder vallen dan de psychologische en psychiatrische gegevens.⁸⁶

Wijze van verzamelen

Een ziekenhuis verzamelt gegevens van haar patiënten op diverse wijzen. Uit de afgenomen interviews kwam het volgende traject naar voren: Een patiënt wordt verwezen naar een arts. Dat is de eerste verwerking; het verwijsbericht. Vervolgens ontvangt de arts voordat de behandeling aanvangt gegevens via het voortraject, via de eerste lijn. De huisarts is namelijk wettelijk verplicht om gegevens uit het dossier van de patiënt aan te leveren bij de specialist. Ook vanuit andere eerste- of tweedelijns behandelaars komt er informatie binnen.⁸⁷ De arts is vervolgens verplicht om te verifiëren of hij voldoende informatie heeft ontvangen om de behandeling uit te voeren. In de wet staat namelijk niet precies aangegeven welke gegevens er aangeleverd moeten worden. Hierbij staat alleen dat het datgene dient te zijn waarvan de arts acht dat hij het nodig heeft. Landelijk zijn er wel afspraken tussen ziekenhuizen over wat het kernsetje van gegevens is wat wordt gegeven als een patiënt wordt doorverwezen. De vorm van deze gegevensuitwisseling is op papier. Behandelaars kunnen dus gewoon een brief meegeven of bijvoorbeeld een CD met röntgenfoto's. Gegevensuitwisseling kan echter ook volledig elektronisch. Dit gaat dan via elektronische brieven.⁸⁸

Wanneer de arts acht voldoende informatie te hebben voor de behandeling is hij nog wettelijk verplicht om te verifiëren of die patiënt daadwerkelijk is wie hij zegt te zijn. Bij wet is geregeld dat men het Burgerservicenummer van een patiënt mag gebruiken om te communiceren tussen zorgverleners. Bij binnenkomst van de patiënt dient het VUmc dus te vragen om Burgerservicenummer en legitimatie. Dit is de eenmalige vaststelling. Daarna

⁸³ Zie interview 1, bijlage V, p. 54

⁸⁴ Zie interview 9, bijlage V, p. 117

⁸⁵ Zie interview 3, bijlage V, p. 72

⁸⁶ Zie interview 1, bijlage V, p. 54

⁸⁷ Zie interview 5, bijlage V, p. 88, interview 9, bijlage V, p. 117-118

⁸⁸ Zie interview 9, bijlage V, p. 117-118

dient een zorgverlener bij ieder contact zich er van vergewissen dat het nog om dezelfde patiënt gaat. Dit wordt in de wet de gewisplicht genoemd. Daarnaast dient de arts alles vast te leggen aan de hand van aantoonbare zaken zoals het verzekeringspasje en de NAW-gegevens. Men kan eventueel een check doen bij de gemeente of de verzekeraar.⁸⁹

Wanneer alle gegevens ingevoerd en gecheckt zijn, krijgt de patiënt een eerste consult bij de arts. Dat verloopt ook eigenlijk altijd standaard. De arts doet dan eerst de zogenaamde anamnese, het vraaggesprek. Hierin wordt gevraagd naar de situatie en naar allerlei andere zaken die de arts wil weten. Al deze gegevens worden genoteerd in het elektronisch patiëntendossier. Vervolgens stelt de arts een soort differentiaal diagnose op. Hierbij kijkt hij naar de mogelijke diagnoses die zouden kunnen horen bij de klachten van de patiënt. Vervolgens plaatst de arts orders voor het doen van aanvullend onderzoek. Dat doet hij om diagnoses uit te sluiten. Op basis van deze aanvullende onderzoeken komt de arts tot een hoofddiagnose en op basis van deze diagnose wordt de therapie ingesteld. De therapie instellen bestaat ook weer uit orders. Bij het vervolgconsult wordt via een zogenaamde decursus de voortgang van de behandeling de resultaten daarvan vastgesteld. Dat is het einde behandeling. De gegevens worden verstuurd naar de verwijzers, dus ook naar de huisarts, om te zorgen dat er continuïteit is van de behandeling. Daarnaast worden de gegevens gebruikt voor allerlei landelijke registraties. In het kader van kwaliteit van zorg dienen alle ziekenhuizen ook allerlei informatie over de kwaliteit van zorg specifiek geënt op patiëntengroepen melden. Wanneer de behandeling volledig ten einde is wordt er een diagnose behandelcombinatie geproduceerd, welke vervolgens aan de verzekering wordt verzonden ter betaling.⁹⁰

Naast dat deze gegevens binnen het VUmc worden verzameld, is het VUmc tevens wettelijk verplicht om een set van deze gegevens te delen met zorgverzekeraars. Niet alle gegevens die bekend zijn binnen het ziekenhuis worden gedeeld met zorgverzekeraars, het gaat hierbij voornamelijk om diagnosecodes, naam en adresgegevens van de patiënt.⁹¹

Doeleinden

Persoonsgegevens van patiënten worden verzameld voor meerdere doeleinden. Uit de interviews kwam naar voren dat het primaire doel van het verzamelen van persoonsgegevens het stellen van diagnoses, het uitvoeren van onderzoek en het instellen van therapieën is. Daarnaast zijn deze gegevens ook van belang voor de continuïteit van de behandeling, voor de kwaliteit van zorg en voor betaling van de zorgverzekeraar.⁹² Hierbij wordt er dus voldaan aan de verplichtingen vanuit de WGBO en de Zorgverzekeringswet.⁹³

⁸⁹ Zie interview 9, bijlage V, p. 117-118

⁹⁰ Zie interview 1, bijlage V, p. 54-55

⁹¹ Zie interview 3, bijlage V, p. 72

⁹² Zie interview 1, bijlage V, p. p. 54-55, interview 3, bijlage V, p. 72, interview 5, bijlage V, p. 89, interview 9, bijlage V, p. 118

⁹³ Zie interview 2, bijlage V, p. 64, interview 3, bijlage V, p. 72

Het secundaire doel is begeleiding van de patiënt tijdens de behandeling maar vooral ook daarna. Dit heeft ook te maken met de privésituatie van de patiënt: Woont de patiënt alleen, heeft hij aanspraak, als hij aanspraak heeft wie is dat dan, is het iemand die de behandelaar erbij kan betrekken? Hierbij gaat het er dus om een beeld te krijgen van hoe de patiënt verder gaat na een medische ingreep. Dit traject begeleidt de specialist vanuit het ziekenhuis samen met de huisarts.⁹⁴

5.1.2 Belang extern privacybeleid

Hoewel het extern privacybeleid een wettelijke verplichting is, is het voor het VUmc ook van belang om te beseffen wat het daadwerkelijke belang is van een dergelijk beleid en waarom een goed beleid nodig is om te voldoen aan de regelgeving van de AVG. Om deze redenen is aan medewerkers de vraag gesteld wat volgens hen het belang is van een extern privacybeleid.

Volgens bijna alle participanten is transparantie het voornaamste belang van een extern privacybeleid.⁹⁵ De AVG versterkt namelijk de rechten van de betrokkenen.⁹⁶ In de AVG zijn zaken verwerkt die gebaseerd zijn op expliciete toestemming van de patiënt voor het vastleggen van gegevens.⁹⁷ Patiënten moeten daarom op de hoogte worden gesteld over de wijze waarop het VUmc privacy waarborgt, welke persoonsgegevens zij verwerkt, waar deze gegevens worden opgeslagen, wie er toegang toe heeft, wat er met die persoonsgegevens wordt gedaan, met welke partijen het VUmc samenwerkt⁹⁸ en dat gegevens op een zorgvuldige wijze worden gearhiveerd.⁹⁹ Het VUmc kan namelijk het intern beleid wel goed op orde hebben, maar het is juist van belang dat patiënten ook weten dat het VUmc het op orde heeft.

Om dit te kunnen waarborgen is het natuurlijk van belang dat het VUmc een extern privacybeleid heeft en dat dit zo transparant mogelijk is en toegankelijk is voor alle soorten patiënten.¹⁰⁰ De informatie moet dus kort, bondig, niet technisch en niet juridisch worden verstrekt.¹⁰¹

Naast het belang van transparantie is het belang van een extern privacybeleid ook het wekken van vertrouwen van de patiënt. De arts-patiënt relatie berust op vertrouwen. Een onderdeel van dat vertrouwen is dat de patiënt er zeker van moet kunnen zijn dat alles wat hij aan een hulpverlener toevertrouwd ook geheim blijft. De Medisch directeur van het AMC

⁹⁴ Zie interview 5, bijlage V, p. 89

⁹⁵ Zie interview 1, bijlage V, p. 55, interview 2, bijlage V, p. 64, interview 3, bijlage V, p. 73, interview 4, bijlage V, p. 82, interview 5, bijlage V, p. 89, interview 7, bijlage V, p. 105, interview 8, bijlage V, p. 111, interview 9, bijlage V, p. 118-119

⁹⁶ Zie interview 1, bijlage V, p. 55

⁹⁷ interview 9, bijlage V, p. 118-119

⁹⁸ Zie interview 2, bijlage V, p. 64, interview 3, bijlage V, p. 73, interview 4, bijlage V, p. 82, interview 5, bijlage V, p. 89, interview 7, bijlage V, p. 105, interview 8, bijlage V, p. 111, interview 9, bijlage V, p. 118-119

⁹⁹ Zie interview 8, bijlage V, p. 111

¹⁰⁰ Zie interview 7, bijlage V, p. 105

¹⁰¹ Zie interview 1, bijlage V, p. 55, interview 9, bijlage V, p. 118-119

ziet het extern privacybeleid dan ook als een vertaling van het beroepsgeheim naar de hele instelling toe.¹⁰²

5.2 Huidig en toekomstig extern privacybeleid

5.2.1 Huidig extern privacybeleid

Om te kunnen bepalen in hoeverre het huidige extern privacybeleid van het VUmc voldoet aan de AVG en welke stappen er nog moeten worden ondernomen om een extern privacybeleid compliant aan de AVG te krijgen, is het van belang om eerst te kijken wat het huidige extern privacy beleid precies inhoudt. Aan de participanten is daarom gevraagd hoe het huidige extern privacybeleid is ingericht, hoe patiënten worden geïnformeerd, hoe er toezicht wordt gehouden, wat hun mening is over het huidige extern privacybeleid en of het voor patiënten duidelijk is waar zij terecht kunnen met hun vragen. Daarnaast is er aan de opdrachtgever gevraagd uit welke documenten het huidige privacybeleid van het VUmc bestaat, is er gekeken naar beschikbare informatie op de website van het VUmc en is er gekeken naar de inhoud en de vindbaarheid van de brochure die het VUmc op dit moment heeft. Deze documenten zijn niet uitvoerig geanalyseerd aangezien dit onderzoek anders te breed zou worden, maar zijn wel opgenomen in de bijlagen ter ondersteuning van de interviews.

Inrichting huidig extern privacybeleid

Uit bijna alle interviews kwam naar voren dat medewerkers eigenlijk niet goed weten wat het huidige extern privacybeleid inhoudt of waar dat te vinden is.¹⁰³ De participanten gaven aan dat zij alleen weten dat het VUmc wel 'iets' over privacy en rechten en plichten op haar website (Bijlage IV) heeft staan¹⁰⁴ en dat zij een brochure genaamd 'Rechten en plichten' (Bijlage III) heeft, maar dat beide niet makkelijk te vinden zijn en het is dus ook niet bekend is of patiënten hier kennis van nemen.¹⁰⁵

Hoewel de informatie op de website en in de folder niet makkelijk te vinden is, worden patiënten ook mondeling geïnformeerd over privacy. Vanuit de WGBO zijn er strenge eisen gesteld aan privacy. In de spreekkamers vragen artsen aan patiënten ook of er specifieke wensen zijn rondom privacy. De artsen hanteren voor dergelijke privacyvragen een checklist, er mag namelijk geen behandelingsovereenkomst worden aangegaan indien de patiënt niet volledig geïnformeerd is. De WGBO stelt geen eisen aan het mondeling of schriftelijk informeren. De vragen worden daarom mondeling gesteld en worden vervolgens in het dossier vastgelegd. Dit is dus niet eenvoudig vindbaar.¹⁰⁶

Ook op het moment dat het VUmc aan een patiënt vraagt of ze zijn gegevens mag gebruiken voor onderzoek, is zij verplicht aan te geven wat zij er mee doet.¹⁰⁷ Tevens worden patiënten

¹⁰² Zie interview 6, bijlage V, p. 97

¹⁰³ Zie interview 1, bijlage V, p. 56, interview 3, bijlage V, p. 73, interview 4, bijlage V, p. 82, interview 6, bijlage V, p. 97-98, interview 7, bijlage V, p. 106

¹⁰⁴ Zie interview 1, bijlage V, p. 56, interview 3, bijlage V, p. 73, interview 7, bijlage V, p. 106, interview 9, bijlage V, p. 119

¹⁰⁵ Zie interview 1, bijlage V, p. 56, interview 3, bijlage V, p. 35

¹⁰⁶ Zie interview 3, bijlage V, p. 73

¹⁰⁷ Zie interview 9, bijlage V, p. 119

geïnformeerd wanneer zij hun dossier opvragen of willen inzien. Hierbij wordt benadrukt dat er een handtekening en een kopie van hun legitimatiebewijs nodig is om vanuit de privacyregelgeving zorgvuldig met de gegevens van de patiënt om te gaan.¹⁰⁸

Naast de informatie via de website, de folder en mondeling worden patiënten ook via 'Mijn dossier' in het EPD geïnformeerd over privacy. Hierin worden medische gegevens van de centrale statusvoering overgeheveld naar de omgeving van de patiënten zelf. De informatie wordt daar aangeboden via links.¹⁰⁹

Uit de interviews kwam naar voren dat het eigenlijke probleem binnen het VUmc is dat er wel informatie over privacy bestaat maar dat dit vooral uit losse flodders bestaat. Er bestaat binnen het VUmc geen document waarin in alle informatie samenkomt en wat 'extern beleid' of 'privacystatement' heet.¹¹⁰ De participanten gaven dan ook aan dat met de komst van de AVG er een duidelijk en prominent¹¹¹ extern privacybeleid moet komen en het privacystatement en het privacybeschermingsbeleid in ieder geval moeten worden afgestemd op de strengere eisen van de AVG. Het VUmc en het AMC zullen op termijn ook een gezamenlijk beleid in gaan hanteren.¹¹²

Toezicht

Aangezien er dus binnen het VUmc op dit moment niet echt sprake is van een eenduidig extern privacybeleid, bestaat er ook geen duidelijk toezicht hierop.¹¹³ De Functionaris Gegevensbescherming en de stafadviseur Privacybescherming en Informatiebeveiliging houden wel toezicht op de informatiebeveiliging, wat een van de vereisten is uit de Wbp. Ook zijn er bepaalde normen waaraan gehouden wordt, zoals de NEN7510 norm voor informatiebeveiliging in de zorg. Het VUmc heeft een Informationsecuritymanagement systeem, een PDCA cyclus op het gebied van privacybescherming en informatiebeveiliging. Vanuit het beleid worden er risico inventarisaties gedaan. Uit deze risico inventarisaties komen beheersmaatregelen. De beheersmaatregelen worden vervolgens opgenomen in het jaarplan. Daarnaast heeft het VUmc een intern auditprogramma. Afdelingen worden geaudit op basis van een aantal vragen die afgeleid zijn van de NEN7510. Uit deze audits komen tekortkomingen naar voren waarna afdelingen een verbeterplan dienen op te stellen. Door middel van een auditprogramma wordt er dus toegezien toe op de naleving van de Wbp. De nadruk van het huidige auditprogramma ligt echter nog op informatiebeveiliging. In de komende jaren zal het gedeelte met betrekking tot privacybescherming worden uitgebreid.¹¹⁴ Het VUmc houdt op dit moment dus met name toezicht op het intern privacybeleid en niet op het externe privacybeleid.

¹⁰⁸ Zie Interview 8, bijlage V, p. 111-112

¹⁰⁹ Zie interview 5, bijlage V, p. 89-90, interview 9, bijlage V, p. 119

¹¹⁰ Zie interview 3, bijlage V, p. 73

¹¹¹ Zie interview 1, bijlage V, p. 56

¹¹² Zie interview 9, bijlage V, p. 119

¹¹³ Zie interview 3, bijlage V, p. 74

¹¹⁴ Zie interview 1, bijlage V, p. 57

Vragen en klachten patiënten

De AVG verplicht organisaties om transparant te zijn tegenover betrokkenen. Patiënten van het VUmc moeten dus ook op de hoogte zijn bij wie zij terecht kunnen met hun vragen over privacy. Om er achter te komen of op dit moment duidelijk is voor patiënten bij wie zij terecht kunnen met hun vragen, of dat hier nog iets aan verbeterd moet worden, is aan de participanten gevraagd of zij denken of het op dit moment voor patiënten duidelijk genoeg is bij wie zij terecht kunnen met hun vragen. Over het algemeen waren de participanten allemaal van mening dat het voor patiënten duidelijk is dat zij met vragen of klachten naar de Servicebalie kunnen gaan.¹¹⁵ Daar worden de eerste vragen behandeld en vindt de eerste klachtopvang plaats.¹¹⁶ de medewerkers die daar werken zijn er op getraind om patiënten te informeren over geheimhouding, privacy en hun rechten.¹¹⁷ Ook weten de patiënten dat zij zich met hun vragen tot hun behandelaar kunnen wenden. De behandelaar zal deze vragen dan doorsturen naar de Servicebalie of naar de Functionaris Gegevensbescherming.¹¹⁸

Hoewel het voor patiënten duidelijk is dat ze terecht kunnen bij de Servicebalie en bij hun behandelaar, zou het voor hen ook bekend moeten zijn dat zij zich met hun vragen rechtevrees tot de Functionaris Gegevensbescherming kunnen wenden.¹¹⁹ Uit de interviews bleek echter dat het voor patiënten niet duidelijk wie de Functionaris Gegevensbescherming is, wat die functie inhoudt, dat hij onafhankelijk is en dat ze zich rechtevrees met een klacht tot hem kunnen wenden. De Functionaris Gegevensbescherming moet dus zichtbaar zijn binnen het ziekenhuis.¹²⁰ De privacyportefeuillehouder gaf aan dat dit kan door bijvoorbeeld een e-mailadres van de Functionaris Gegevensbescherming op de website van het VUmc te plaatsen.¹²¹ De Functionaris Gegevensbescherming van het VUmc gaf echter zelf aan dat het wel bekend moet zijn maar dat hij liever heeft dat patiënten zich eerst tot de Servicebalie wenden.¹²²

Mening extern privacybeleid

Naar aanleiding van de vragen over de inrichting van het huidige extern privacybeleid, is aan de werknemers gevraagd wat zij zelf vinden van het huidige beleid en of zij van mening zijn dat er iets veranderd moet worden. Ook deze vraag is gesteld om bewustwording te creëren binnen het VUmc en werknemers zelf na te laten denken over het nut van een goed extern privacybeleid.

Een deel van de participanten was van mening dat het huidige extern privacybeleid voldoende is.¹²³ De Servicebalie krijgt weinig vragen van patiënten die verontrust zijn over privacy en

¹¹⁵ Zie interview 2, bijlage V, p. 65, interview 3, bijlage V, p. 74, interview 5, bijlage V, p. 92, interview 6, bijlage V, p. 100, interview 7, bijlage V, p. 106, interview 8, bijlage V, p. 112

¹¹⁶ Zie interview 2, bijlage V, p. 65, interview 3, bijlage V, p. 74-75, interview 5, bijlage V, p. 92, interview 6, bijlage V, p. 100, interview 7, bijlage V, p. 106

¹¹⁷ Zie interview 3, bijlage V, p. 74-75

¹¹⁸ Zie interview 5, bijlage V, p. 92, interview 6, bijlage V, p. 100

¹¹⁹ Zie interview 1, bijlage V, p. 58, interview 2, bijlage V, p. 65, interview 4, bijlage V, p. 83

¹²⁰ Zie interview 1, bijlage V, p. 58, interview 2, bijlage V, p. 65, interview 4, bijlage V, p. 83

¹²¹ Zie interview 4, bijlage V, p. 83

¹²² Zie interview 1, bijlage V, p. 58

¹²³ Zie interview 5, bijlage V, p. 91, interview 6, bijlage V, p. 100, interview 8, bijlage V, p. 112

dat vinden zij een graadmeter.¹²⁴ De meeste communicatie met patiënten loopt bij het VUmc decentraal. Op het moment dat een patiënt wordt opgenomen of de polikliniek bezoekt, krijgt hij een brief vanuit de afdeling. Waarschijnlijk scheelt het per afdeling hoe goed de informatievoorziening op orde is.¹²⁵ Patiënten hebben echter al veel algemene informatie over hoe er met privacy hoort te worden omgegaan¹²⁶ en gaan er vanuit dat het binnen het VUmc op orde is.¹²⁷ Ook weet een deel van de patiënten goed wat hun rechten zijn.¹²⁸ Patiënten hoeven daar dus volgens de Medisch directeur niet extra over ingelicht te worden.¹²⁹ Volgens de communicatieadviseur van het VUmc is het de kunst op om het moment dat een patiënt vragen heeft, de informatie op het juiste moment in het proces aan te bieden. Informatie moet dus pas worden aangeboden op het moment dat het voor een patiënt relevant is. Op het moment dat een patiënt wordt opgenomen moet het volgens de communicatieadviseur in hapklare brokken worden geven. Dit kan bijvoorbeeld door middel van het in een korte alinea aangeven wat het VUmc doet op het gebied van privacy en dat de patiënten die er dan meer over willen weten kunnen doorklikken.¹³⁰

De stafadviseur Privacybescherming en Informatiebeveiliging van het VUmc gaf aan dat zij van mening is dat het extern privacybeleid onder de huidige wet voldoende is, maar dat het met de komst van de AVG niet voldoende is. Toekomstgericht is het huidige beleid dus niet meer toereikend. Met de komst van de AVG moet het VUmc patiënten gaan vertellen welke gegevens het VUmc van patiënten heeft, wat zij met die gegevens doet en waarom. Hierbij gaf de adviseur aan dat hoewel het een wettelijke plicht is, zij zich afvraagt of het ook de behoefte van de patiënt is.¹³¹

De Functionaris Gegevensbescherming van het VUmc gaf daarentegen aan dat hij de wijze waarop patiënten onder het huidige beleid worden geïnformeerd niet voldoende vindt. Hij is van mening dat het een tekortkoming is dat het huidige extern beleid niet te vinden is op de website. Patiënten moeten helder en snel kunnen vinden hoe het VUmc met persoonsgegevens omgaat.¹³² Ook de businessanalist denkt dat het extern privacybeleid beter kan. Wat hem betreft heeft de AVG dan ook een goede slag maakt door te verplichten dat het een simpele, leesbare tekst moet zijn en er geen juridische termen in mogen staan. Het huidige voorlichtingsmateriaal over privacy en de klachtencommissies waar patiënten binnen kunnen stappen met hun vragen, zijn niet voldoende volgens hem. Via het EPD worden patiënten wel voldoende voorgelicht over privacy. Wat hem betreft kunnen alleen de teksten die daarop staan nog aangepast worden ter verbetering. Wel gaf hij aan dat het VUmc op dit

¹²⁴ Zie interview 8, bijlage V, p. 112

¹²⁵ Zie interview 7, bijlage V, p. 106

¹²⁶ Zie interview 6, bijlage V, p. 99

¹²⁷ Zie interview 7, bijlage V, p. 106

¹²⁸ Zie interview 5, bijlage V, p. 91

¹²⁹ Zie interview 6, bijlage V, p. 99

¹³⁰ Zie interview 7, bijlage V, p. 106

¹³¹ Zie interview 3, bijlage V, p. 74

¹³² Zie interview 1, bijlage V, p. 57-58

moment NEN7510 gecertificeerd is en daarmee al wel een goede stap heeft gemaakt richting de AVG.¹³³

5.2.2 Extern privacybeleid onder de AVG

Zoals uit paragraaf 5.3 naar voren kwam zijn veel medewerkers niet op de hoogte van de precieze inrichting van het huidige extern privacybeleid van het VUmc. Aan de participanten is daarom gevraagd welke aanpassingen gedaan moeten worden aan het huidige extern privacybeleid voor een AVG compliant extern privacybeleid.

Uit de interviews blijkt dat het voornamelijk van belang is dat het VUmc gaat voldoen aan de informatieplicht.¹³⁴ Het VUmc moet haar patiënten conform artikel 13 en 14 gaan informeren over alle verwerkingen van persoonsgegevens, dus niet alleen patiëntgegevens, maar ook gegevens van de website, kentekens en het gebruik van camera's.¹³⁵ Daarnaast is het van belang om patiënten te informeren dat het VUmc vanuit een netwerk van subcontractors werkt die bepaalde zaken van haar overnemen, maar dat het VUmc er op toeziet dat de kwaliteit en privacy hetzelfde is als bij haar. Voor het vertrouwen van de patiënt is het van belang dat zij hier goed over geïnformeerd worden¹³⁶. Bij het opstellen van het extern privacybeleid dient het VUmc dus naast de patiënt te gaan staan, de AVG er naast te leggen en vervolgens vanuit die positie te gaan kijken wat het VUmc moet doen om te voldoen aan de informatieplicht.¹³⁷ Daarnaast moet het VUmc een privacystatement opstellen en de huidige folder aanpassen.¹³⁸

5.3 Communicatiekanalen extern privacybeleid

5.3.1 Algemeen

Zoals in paragraaf 4.6 naar voren kwam, zegt de AVG niet expliciet iets over hoe een extern privacybeleid moet worden gecommuniceerd naar betrokkenen. Artikel 12 AVG schrijft slechts voor dat de informatie over gegevensverwerking in een gemakkelijk toegankelijke vorm verstrekt dient te worden. Zoals in paragraaf 4.6 onderzocht betekent 'gemakkelijk toegankelijk' volgens Werkgroep 29 dat de betrokkenen de informatie niet op hoeven te zoeken, maar dat het voor hen direct duidelijk is waar zij deze informatie kunnen vinden.

Aangezien de afdeling Communicatie dagelijks bezig is met het op een zo aantrekkelijk mogelijk overbrengen van informatie aan patiënten, is aan de communicatieadviseur van het VUmc gevraagd hoe een extern privacybeleid volgens hem zou moeten worden gecommuniceerd naar patiënten zodat het voor hen makkelijk toegankelijk is. Hij gaf aan dat het belangrijk is om te beseffen dat privacy niet het eerste waar patiënten mee bezig zijn. Patiënten komen in eerste instantie voor zorg, en privacy is een basisvoorwaarde. Patiënten

¹³³ Zie interview 9, bijlage V, p. 119-120

¹³⁴ Zie interview 2, bijlage V, p. 67, interview 5, bijlage V, p. 93

¹³⁵ Zie interview 2, bijlage V, p. 67

¹³⁶ Zie interview 5, bijlage V, p. 93

¹³⁷ Zie interview 4, bijlage V, p. 85

¹³⁸ Zie interview 2, bijlage V, p. 67, interview 3, bijlage V, p. 78

gaan er dus van uit dat privacy goed geregeld is binnen het VUmc. Volgens de communicatieadviseur moet er in ieder geval een statement op de website moet komen. Hierbij is het van belang dat het VUmc dit statement ook presenteert op een manier die patiënten begrijpen. Het moet leesbaar zijn. Het mag geen juridische tekst zijn maar het moet echt op B1 niveau worden geschreven, zodat het voor iedereen begrijpelijk is. Hierbij kan ook gedacht worden aan een samenvatting van een juridische tekst in een nieuwsbericht. Volgens de communicatieadviseur is ook het inzetten van socialkanalen erg belangrijk voor het besteden van aandacht aan het nieuwe privacybeleid. Het VUmc is actief op Facebook, LinkedIn, Instagram en Twitter. Per kanaal moet de boodschap op het publiek worden aangepast en dus anders worden overgebracht. Via Facebook kan dit volgens hem bijvoorbeeld door middel van korte vragen en antwoorden.¹³⁹

Volgens de voorzitter van de Cliëntenraad weegt het communicatietraject van het extern privacybeleid erg zwaar. Het is van belang dat het VUmc zo transparant mogelijk is in haar informatievoorziening en dat patiënten op verscheidene wijzen aan informatie kunnen komen.¹⁴⁰ Er moet dus onderzocht worden wat de belangrijkste poorten van patiënten tot het ziekenhuis zijn. Op die plekken moet de informatie worden aangeboden.¹⁴¹ Uit de andere interviews werd duidelijk dat het extern privacybeleid daarom te vinden moet zijn in My Chart, via een privacystatement op de website van het VUmc, in folders en in Narrow Casting.¹⁴² Daarnaast moet er in de zorgovereenkomst een aantal zinnen worden opgenomen over privacy¹⁴³ en moet er informatie over het beleid in patiëntenbrieven komen.¹⁴⁴ Dit moet zo simpel mogelijk, bijvoorbeeld door middel van het beantwoorden van vragen in bulletpoints. Deze informatie dient tevens toegankelijk te worden gemaakt voor gehandicapten die niet goed kunnen zien of horen.¹⁴⁵ Een volgende optie is om patiënten een DVD of een stick mee te geven waar meer informatie over het privacybeleid op te vinden is.¹⁴⁶ Hoewel folders wel genoemd worden als communicatiekanaal, bestaan er nog wel meningsverschillen over het werkelijke belang hiervan. De privacyportefeuillehouder denkt dat folders niet zoveel zin hebben aangezien patiënten folders toch niet lezen. Volgens haar zijn de folders er alleen maar om aan de AVG te voldoen, maar is dit communicatiekanaal maximaal 5 procent van het hele beleid.¹⁴⁷ De voorzitter van de Cliëntenraad is van mening dat het grootste gedeelte van de bevolking juist niet via elektronica geïnformeerd wil worden, maar juist liever een folder leest. De medewerker van de Servicebalie gaf aan dat folders én digitaal én op papier te verkrijgen moeten zijn. Zo sluit het VUmc aan op de jongere groep

¹³⁹ Zie interview 7, bijlage V, p. 107

¹⁴⁰ Zie interview 3, bijlage V, p. 76-77, interview 5, bijlage V, p. 94, interview 8, bijlage V, p. 114

¹⁴¹ Zie interview 3, bijlage V, p. 77

¹⁴² Zie interview 1, bijlage V, p. 60, interview 2, bijlage V, p. 68, interview 3, bijlage V, p. 77, interview 4, bijlage V, p. 85, interview 8, bijlage V, p. 114-115

¹⁴³ Zie interview 4, bijlage V, p. 85

¹⁴⁴ Zie interview 7, bijlage V, p. 107, interview 8, bijlage V, p. 114

¹⁴⁵ Zie interview 2, bijlage V, p. 68

¹⁴⁶ Zie interview 5, bijlage V, p. 94

¹⁴⁷ Zie interview 4, bijlage V, p. 85

patiënten die men beter met het internet bereikt, en op de groep met oudere patiënten die meer baat hebben bij een folder.

Voordat het extern privacybeleid wordt gepresenteerd moet echter het intern privacybeleid eerst op orde zijn. Medewerkers moeten voorbereid zijn op eventuele vragen die zij gaan krijgen. Op dit moment worden medewerkers middels een campagne voorbereid op de AVG.¹⁴⁸ Ook moet het extern privacybeleid in gedragscodes voor werknemers komen te staan, autorisaties moeten helder ingericht zijn en het moet duidelijk zijn dat het gaat over privacy.¹⁴⁹

5.3.2 Specifiek- Privacystatement

In paragraaf 4.6 werd duidelijk dat de AVG geen duidelijke eisen stelt aan de manier waarop het extern privacybeleid verstrekt moet worden. Uit deze paragraaf bleek echter dat Werkgroep 29 het advies geeft om in ieder geval een privacystatement op te stellen. Aan de participanten zijn daarom vragen voorgelegd met betrekking tot de inhoud, het taalgebruik, de vormgeving en de plaats (vindbaarheid op de website) van het privacystatement van het VUmc.

Inhoud

In paragraaf 4.4 is onderzocht welke eisen de AVG stelt aan de inhoud van een extern privacybeleid, wat dus onder meer vertaald dient te worden in een privacystatement. Om een volledig beeld te krijgen van de invulling van het privacystatement van het VUmc, is aan de participanten gevraagd welke onderwerpen het privacystatement volgens hen in ieder geval moet bevatten. Hier is onderscheid gemaakt tussen onderwerpen die de participanten zelf aandroegen en de behoefte die er volgens de participanten vanuit de patiënten is naar de inhoud van het privacystatement.

Het eerste doel van een privacystatement is volgens de Functionaris Gegevensbescherming van het VUmc dat patiënten weten hoe het VUmc met privacy omgaat. Het tweede doel is het wekken van het vertrouwen van deze patiënten. Het privacystatement dient volgens hem dan ook de volgende onderwerpen te bevatten: Ten eerste moet in twee alinea's worden verteld hoe VUmc omgaat met privacy. Vervolgens moet worden verteld welke gegevens het VUmc verzameld en verwerkt, voor welke doelen zij dat doet en dat zij dat niet meer doet dan noodzakelijk. Tevens moet worden verteld wat er met deze gegevens wordt gedaan, dit kan dan gekoppeld worden aan de doelstelling van de verwerking. De vierde poot is aan wie het VUmc de gegevens doorgeeft. Patiënten moeten op de hoogte worden gesteld dat gegevens naar de huisarts en naar andere verwijzers worden verzonden, maar ook dat VUmc gegevens aan landelijk verplichte registraties levert. Vervolgens moet worden verteld wat de rechten van de patiënten zijn en hoe deze uitgeoefend kunnen worden. Alle patiëntenrechten moeten in het privacystatement worden vermeld, met een doorklik naar wat meer informatie. Tevens

¹⁴⁸ Zie interview 3, bijlage V, p. 78, interview 7, bijlage V, p. 107

¹⁴⁹ Zie interview 4, bijlage V, p. 85

moet in het privacystatement komen te staan welke stappen patiënten kunnen nemen indien ze klachten of vragen hebben. Patiënten kunnen hiervoor namelijk terecht bij de Servicedesk.¹⁵⁰

Uit de andere interviews kwam naar voren dat er in ieder geval in het statement moet komen te staan wat de identiteit is van de organisatie, wie de Functionaris Gegevensbescherming is, wat het doel is van de organisatie, welke gegevens het VUmc van de patiënt verwerkt (ook bij gebruik van de website), voor welke doelen, wie toegang hebben tot de gegevens, of het VUmc de gegevens beveiligt, hoelang de gegevens bewaard worden, hoe de patiënten hun rechten kunnen uitoefenen en waar patiënten terecht kunnen met klachten.¹⁵¹ Dit dient kort en krachtig vermeld te worden.¹⁵² Hierbij is het van belang om te benadrukken dat met alle gegevens van de patiënt die binnen het VUmc verwerkt worden vertrouwelijk wordt omgegaan en dat die gegevens niet zomaar het ziekenhuis kunnen verlaten of dat die gegevens niet worden doorgegeven naar zorgverzekeraars.¹⁵³

De Functionaris Gegevensbescherming van het AMC gaf tevens aan dat men in een privacystatement ook moet voldoen aan de Telecommunicatiewet. In het privacystatement moet de organisatie ook iets kunnen vertellen over het automatisch verwerken van gegevens en dat de organisatie het IP-adres van personen verwerkt. Ook dient men te vertellen of de organisatie cookies of soortgelijke technieken gebruikt.¹⁵⁴

Inrichting en taalgebruik

Uit paragraaf 4.3 kwam naar voren dat de AVG strenge eisen stelt aan het taalgebruik dat gehanteerd dient te worden in het extern privacybeleid of het privacystatement. Artikel 12 lid 1 AVG stelt namelijk de eis dat deze informatie op een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal verstrekt dient te worden. Daarnaast bleek dat de AVG verplicht stelt dat deze informatie ook voor kinderen begrijpelijk is. Wanneer de verwerking specifiek tot een kind gericht is, dient de informatie en communicatie in een zodanig duidelijke en eenvoudige taal te worden opgesteld dat het kind deze makkelijk kan begrijpen.

Hoewel het dus duidelijk is dat het taalgebruik zeer eenvoudig dient te zijn, is aan de participanten gevraagd hoe de informatie in het privacystatement van het VUmc zou moeten worden opgesteld zodat het aan deze eis voldoet, en of er volgens hen juridische gevaren schuilen in het gebruik van eenvoudige taal.

Uit de interviews met de Functionaris Gegevensbescherming van het VUmc, de stafadviseur Privacybescherming en Informatiebeveiliging en de Privacyportefeuillehouder blijkt dat zij van mening zijn dat er geen gevaren schuilen in een privacystatement in begrijpelijke taal. De

¹⁵⁰ Zie interview 1, bijlage V, p. 61

¹⁵¹ Zie interview 2, bijlage V, p. 68, interview 3, bijlage V, p. 79, interview 4, bijlage V, p. 85, interview 6, bijlage V, p. 102, interview 8, bijlage V, p. 115, interview 9, bijlage V, p. 122

¹⁵² Zie interview 3, bijlage V, p. 79

¹⁵³ Zie interview 8, bijlage V, p. 115

¹⁵⁴ Zie interview 2, bijlage V, p. 68

AVG stelt namelijk de eis dat het juist niet juridisch mag zijn. Er mogen dus geen ingewikkelde terminologieën worden gebruikt. Wanneer het VUmc juridische teksten zou gaan publiceren is het risico veel groter dat de boodschap niet overkomt. Juist door kort en krachtig te beschrijven en aan te sluiten op de doelgroep, voldoet het VUmc aan de AVG. De kracht is dus om alle onderwerpen aan bod te laten komen. Indien patiënten daarna nog vragen hebben kunnen ze deze stellen, of kunnen ze verder de diepte in naar meer informatie. De volgorde van informatievoorziening is dan een statement op de website, het register, reglementen van het VUmc en tot slot een toelichting door de FG.¹⁵⁵

Uit andere interviews blijkt dat het statement in Jip en Janneke taal dient te worden geschreven.¹⁵⁶ Ook laaggeletterden en mensen met een beperkt zicht moeten het begrijpen.¹⁵⁷ Dit kan het VUmc controleren door bijvoorbeeld een stuk op te stellen en dit bespreken met een achtjarige. Indien deze achtjarige niet begrijpt wat er staat, dient het aangepast te worden. Kinderen moeten het namelijk ook kunnen begrijpen.¹⁵⁸ Hoewel de AVG spreekt over aparte voorlichting voor kinderen, vraagt de medewerker van de Servicebalie zich af in hoeverre dit zinlijk is. Hij is van mening dat dit niet specifiek nodig is.¹⁵⁹

Uit het merendeel van de interviews kwam ook naar voren dat het van belang is om een gelaagd statement op te stellen. Hierbij werd aangegeven dat dit bijvoorbeeld kan door middel van allereerst een kort privacystatement in begrijpelijke taal met daarin de mogelijkheid om door te klikken naar het externe privacybeleid, wat dan wat uitgebreider en juridisch complexer is.¹⁶⁰ De Privacyportefeuillehouder en de voorzitter van de Cliëntenraad zijn van mening dat hierdoor de aansprakelijkheden beter worden verdeeld en het VUmc zich juridisch beter kan indekken.¹⁶¹

De Functionaris Gegevensbescherming van het AMC en de voorzitter van de Cliëntenraad zijn van mening dat er wel een spanningsveld is als men juridische zaken in begrijpelijke taal wilt brengen.¹⁶² De Functionaris Gegevensbescherming van het AMC gaf aan dat juridische zinnen meestal kort geformuleerd zijn en wanneer men dit om gaat zetten in begrijpelijk taal dat betekent dat het statement meer tekst zal bevatten. Volgens de Functionaris moeten er meer onderwerpen worden uitgeschreven maar mogen er niet minder begrippen worden gebruikt. Dit brengt weer spanning met zich mee aangezien het statement dan teveel tekst zal bevatten. Het belangrijkste is volgens haar echter dat men kijkt naar de rechten en de informatieplichten van de AVG, en dat men daarop steelt.¹⁶³

¹⁵⁵ Zie interview 1, bijlage V, p. 61, interview 3, bijlage V, p. 79, interview 4, bijlage V, p. 85

¹⁵⁶ Zie interview 4, bijlage V, p. 86, interview 6, bijlage V, p. 103

¹⁵⁷ Zie interview 7, bijlage V, p. 108

¹⁵⁸ Zie interview 4, bijlage V, p. 86

¹⁵⁹ Zie interview 8, bijlage V, p. 113

¹⁶⁰ Zie interview 1, bijlage V, p. 61-62, interview 4, bijlage V, p. 86, interview 5, bijlage V, p. 95, interview 7, bijlage V, p. 108, interview 8, bijlage V, p. 115

¹⁶¹ Zie interview 4, bijlage V, p. 86, interview 5, bijlage V, p. 95

¹⁶² Zie interview 2, bijlage V, p. 68-69, interview 5, bijlage V, p. 95

¹⁶³ Zie interview 2, bijlage V, p. 68-69

Vormgeving

Zoals onderzocht in paragraaf 4.5 dient het VUmc passende maatregelen te nemen om informatie aan betrokkenen in ieder geval op een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal te verstrekken.

Werkgroep 29 geeft als advies dat de informatievoorziening beknopt, transparant en op efficiënte wijze moet worden gepresenteerd. Dit kan bijvoorbeeld middels een gelaagd privacystatement. In paragraaf 4.5 bleek dat de informatieverstrekking in ieder geval schriftelijk dient te zijn en dat er daarnaast ook aanvullende visualisatie gebruikt mag worden. Om een beeld te krijgen hoe deze wetgeving en adviezen van het Werkgroep 29 het beste kunnen worden toegepast op het privacystatement van het VUmc, is aan de participanten de vraag voorgelegd hoe zij denken over de vormgeving van het privacystatement.

Uit de interviews bleek dat het met name van belang is om het privacystatement aan te sluiten op alle leeftijden en intelligentieniveaus van de patiënten en dat het dus toegankelijk dient te zijn voor alle patiënten.¹⁶⁴ Daarom dient het statement allereerst in het Nederlands, in het Engels en in een aantal gangbare talen worden opgezet. In de omgeving van het VUmc zijn namelijk veel Turken en Marokkanen woonachtig.¹⁶⁵ Daarnaast was het grootste gedeelte van de participanten van mening dat het erg van belang is om visualisatie te gebruiken bij het privacystatement, aangezien alleen een stuk tekst mensen niet voldoende aanspreekt.¹⁶⁶ Een aantal participanten is van mening dat het gebruik van een filmpje een erg goede manier om het extern privacybeleid te presenteren. Hiermee kan het VUmc zich positief onderscheiden. Patiënten zouden dan moeten kunnen kiezen of ze het beleid willen zien in een filmpje of willen lezen in een tekst, of dat ze na het filmpje door kunnen klikken naar tekst.¹⁶⁷ Bij die tekst kunnen ondersteunende illustraties of pictogrammen worden gebruikt.¹⁶⁸ Een andere optie die werd genoemd is om een grafisch document met bijvoorbeeld pictogrammen, tekeningen of stripverhalen te gebruiken.¹⁶⁹ Hierbij dient in ieder geval gebruik te worden gemaakt van een gelaagde structuur. Een eerste optie hierbij is dat men begint met de basis, de kern die in ieder geval iedereen begrijpt, vervolgens een stuk tekst met pictogrammen voor de patiënten die iets meer informatie willen, en tot slot een volledige tekst.¹⁷⁰ Een tweede optie hierbij is een A-5je met verwijzingen. In het statement moeten dan de allerbelangrijkste onderwerpen worden benoemd met daarbij links naar een korte verklaring over dat specifieke onderwerp.¹⁷¹

De Functionaris Gegevensbescherming van het AMC en de Directeur Medische Zaken van het AMC waren wat kritischer tegenover het gebruik van pictogrammen. Zij gaven aan dat er op

¹⁶⁴ Zie interview 1, bijlage V, p. 61, interview 3, bijlage V, p. 79, interview 7, bijlage V, p. 108, interview 9, bijlage V, p. 122-123

¹⁶⁵ Zie interview 1, bijlage V, p. 61-62

¹⁶⁶ Zie interview 1, bijlage V, p. 62, interview 3, bijlage V, p. 79, interview 4, bijlage V, p. 86, interview 5, bijlage V, p. 57, bijlage V, p. 103, interview 7, bijlage V, p. 108, interview 8, bijlage V, p. 115

¹⁶⁷ Zie interview 1, bijlage V, p. 62, interview 4, bijlage V, p. 86, interview 8, bijlage V, p. 115

¹⁶⁸ Zie interview 1, bijlage V, p. 62

¹⁶⁹ Zie interview 3, bijlage V, p. 79, interview 5, bijlage V, p. 95

¹⁷⁰ Zie interview 4, bijlage V, p. 86, interview 5, bijlage V, p. 95, interview 7, bijlage V, p. 108

¹⁷¹ Zie interview 6, bijlage V, p. 103, interview 8, bijlage V, p. 115

dit moment nog niet gewerkt kan worden met icoontjes of afbeeldingen aangezien die nog niet herkenbaar zijn voor iedereen. Icoontjes hebben namelijk de bedoeling dat wanneer men dat icoontje ziet, geen tekst meer hoeft te worden gelezen. Hier zouden dan afspraken over moeten worden gemaakt. Pas wanneer er icoontjes ontstaan waarvan men kan zeggen dat de gemiddelde Nederlander ze begrijpt, kan er gebruik worden gemaakt van icoontjes. De Functionaris Gegevensbescherming van het AMC is wel van mening dat men gebruik kan maken van matrixen. Hierdoor kan men bijvoorbeeld kort aangeven welke persoonsgegevens bij welke dienst horen, hoe het gedeeld wordt en hoelang het bewaard wordt.¹⁷²

Volgens de Functionaris Gegevensbescherming van het VUmc moet uit het privacystatement in ieder geval blijken dat het VUmc privacy serieus neemt. Wanneer het VUmc dat laat zien door middel van een filmpje, een stuk tekst met illustraties en extra informatie waardoor patiënten verder de diepte in kunnen, laat het VUmc volgens de Functionaris aan de buitenwereld zien dat zij privacy serieus neemt. 'Natuurlijk gaan wij goed om met uw privacy, maar als er toch iets fout gaat krijgen we dat graag van u gemeld'.¹⁷³ Het VUmc kan hierdoor volgens de Privacyportefeuillehouder echt een voorloper worden op dit gebied waardoor patiënten kiezen voor het VUmc omdat zij heel zorgvuldig met persoonsgegevens omgaat.¹⁷⁴

Behoeft patiënten invulling privacystatement

Aangezien het privacystatement op grond van de AVG duidelijk en begrijpelijk dient te zijn voor de betrokkenen, is het van belang om te weten hoe patiënten van het VUmc denken over de invulling van het privacystatement. Er is aan de opdrachtgever gevraagd of er een enquête kon worden afgenomen onder patiënten, om zo hun visie op het privacystatement mee te nemen in dit onderzoek. Dit was wel mogelijk, maar hierdoor zou het onderzoek te uitgebreid worden. Er is daarom besloten om geen enquête uit te voeren. Om toch de visie van patiënten mee te kunnen nemen in dit onderzoek is aan de participanten gevraagd wat zij denken wat de behoefte is van patiënten naar de invulling van het privacystatement.

Alle participanten aan wie deze vraag is voorgelegd antwoordden dat zij denken dat patiënten geen duidelijke mening hebben over dit onderwerp.¹⁷⁵ Over het algemeen is het een aanname van patiënten dat de gegevensverwerking en privacy goed geregeld is, en het VUmc heeft daarom de verantwoordelijkheid om het goed op orde te hebben.¹⁷⁶ Pas op het moment dat er iets mis gaat of er iets over in het nieuws komt, gaan patiënten hier informatie over opzoeken.¹⁷⁷ Het is daarom van belang dat er een privacystatement wordt opgezet die voldoet aan de wet; leesbaar, niet juridisch, niet technisch en met een mooie vormgeving. Wanneer daar reacties op komen van patiënten kan het VUmc het statement aanpassen. Allereerst dient het privacystatement wel uitgezet te worden onder een aantal patiënten om te kijken

¹⁷² Zie interview 2, bijlage V, p. 69-70, interview 6, bijlage V, p. 103

¹⁷³ Zie interview 1, bijlage V, p. 62

¹⁷⁴ Zie interview 4, bijlage V, p. 86

¹⁷⁵ Zie interview 1, bijlage V, p. 62, interview 4, bijlage V, p. 86, interview 5, bijlage V, p. 95-96, interview 7, bijlage V, p. 108-109, interview 9, bijlage V, p. 123

¹⁷⁶ Zie interview 7, bijlage V, p. 108-109

¹⁷⁷ Zie interview 4, bijlage V, p. 86, interview 5, bijlage V, p. 95-96, interview 7, bijlage V, p. 108-109

wat hun mening is hierover en of de informatie duidelijk is. Wanneer deze feedback positief is kan het statement worden gebruikt.¹⁷⁸ Patiënten willen volgens de voorzitter van de Cliëntenraad in ieder geval de rode draad in het verhaal kunnen waarnemen. De belangrijkste zaken moeten naar voren springen.¹⁷⁹

Plaats/vindbaarheid op de website

In paragraaf 4.7 bleek dat organisaties verplicht zijn om betrokkenen op diverse momenten in te lichten over gegevensverwerking en privacy. Een van de momenten waarop dit dient te gebeuren is wanneer het privacybeleid van een organisatie wijzigt. Aangezien er met de komst van de AVG een volledig nieuw privacystatement wordt opgesteld, is het VUmc verplicht haar patiënten daar actief over te informeren. De vraag die hieruit voortvloeit is op welke wijze het VUmc haar patiënten hier het beste over kan informeren. Deze vraag is voorgelegd aan de participanten.

Een tweetal participanten gaven aan dat het van belang is om in de beginperiode duidelijk als een banner of als 'nieuws van de dag' op de website aan te geven dat het VUmc een nieuw privacystatement heeft.¹⁸⁰ Andere participanten gaven aan dat het op de website wel goed vindbaar moet zijn maar dat het niet overduidelijk aanwezig hoeft te zijn.¹⁸¹ Het is niet de primaire taak van het VUmc om aan privacy te voldoen aangezien zij een zorgverlener is.¹⁸² Patiënten moeten niet wanneer zij op zoek zijn naar iets anders worden lastiggevallen met een privacystatement. Het VUmc vindt privacy echter wel heel belangrijk.¹⁸³ Op de website zou onder het kopje 'Patiënteninformatie' het onderwerp 'Privacy' moeten staan en daar zou ook direct het privacystatement te vinden moeten zijn.¹⁸⁴ Een andere optie is om helemaal onderaan de website een kopje met 'Privacystatement' neer te zetten. Patiënten kunnen zo dit kopje altijd blijven zien, waar ze ook heen gaan op de website.¹⁸⁵ De derde optie is om het privacystatement via een link op de website aan te bieden.¹⁸⁶ Ook zou het privacystatement onder het kopje 'Rechten en plichten' te vinden moeten zijn.¹⁸⁷

In het interview met de communicatieadviseur kwam naar voren dat het privacystatement volgens hem niet het eerste moet zijn wat patiënten zien wanneer ze op de homepage komen, maar dat het statement wel op plekken moet komen waar mensen het verwachten. In het interview gaf de communicatieadviseur aan dat het VUmc zich dus moet afvragen waar patiënten in de reis die ze doorlopen op de website vragen kunnen hebben over privacy. Op die plekken moet het VUmc het statement op de juiste manier aanbieden. Volgens hem is het privacystatement ook niet het eerste wat patiënten willen zien. De communicatieadviseur gaf

¹⁷⁸ Zie interview 1, bijlage V, p. 62

¹⁷⁹ Zie interview 5, bijlage V, p. 96

¹⁸⁰ Zie interview 4, bijlage V, p. 86-87, interview 8, bijlage V, p. 115

¹⁸¹ Zie interview 3, bijlage V, p. 79-80, interview 6, bijlage V, p. 103, Zie interview 7, bijlage V, p. 109, interview 9, bijlage V, p. 123

¹⁸² Zie interview 3, bijlage V, p. 79-80, interview 6, bijlage V, p. 103

¹⁸³ Zie interview 3, bijlage V, p. 79-80

¹⁸⁴ Zie interview 1, bijlage V, p. 62, interview 8, bijlage V, p. 115

¹⁸⁵ Zie interview 3, bijlage V, p. 79-80, interview 4, bijlage V, p. 86-87

¹⁸⁶ Zie interview 5, bijlage V, p. 96

¹⁸⁷ Zie interview 6, bijlage V, p. 103

aan dat het VUmc tevens verplicht is om een privacystatement over cookies op haar website te plaatsen en dat wanneer een patiënt daarin geïnteresseerd is, het ook aannemelijk is dat die patiënt in meer privacygerelateerde zaken geïnteresseerd is. Bij het statement over cookies zou het VUmc dus een link kunnen zetten naar het privacystatement voor de hele organisatie'.¹⁸⁸

5.3.3. Specifiek- Folders

Uit paragraaf 4.6 bleek dat het gebruik van folders een van de communicatiekanalen is waardoor het extern privacybeleid verstrekt kan worden. Op dit moment heeft het VUmc niet een folder, maar een brochure genaamd 'Rechten en plichten' (zie bijlage III). Deze folder bestaat uit tekst wat onderverdeeld is in zes hoofdstukken en is gebaseerd op de WGBO. Aan de participanten is gevraagd hoe de folders of brochures met betrekking tot het nieuwe extern privacybeleid moeten worden ingericht zodat ook deze voldoen aan de regelgeving van de AVG.

Uit de interviews kwamen eigenlijk twee opties naar voren. De eerste optie is dat in de folders dezelfde tekst als in het privacystatement wordt opgenomen.¹⁸⁹ De vormgeving dient hierbij wel anders te zijn.¹⁹⁰ Dit kan bijvoorbeeld door middel van het gebruik van plaatjes om zo de folder wat te verlevendigen. De nieuwe folder moet in ieder geval meer beeldend en creatiever dan de huidige folder.¹⁹¹

De tweede optie is dat er in de folders korte en bondige informatie komt te staan met een verwijzing naar de website voor het privacystatement en meer verdieping.¹⁹² In de folder dient dan vermeld te worden wie de Functionaris Gegevenbescherming is en hoe hij te bereiken is.¹⁹³

Het is niet bekend of de huidige folder 'Rechten en plichten' op alle afdelingen ligt.¹⁹⁴ De nieuwe folders moeten wel op alle afdelingen in de wachtkamers komen te staan.¹⁹⁵

5.4 Uitvoering en toezicht extern privacybeleid

5.4.1 Uitvoering door medewerkers

Een goed extern privacybeleid staat of valt met de uitvoering van de medewerkers van het VUmc. Om deze reden is er aan de participanten gevraagd op welke wijze de medewerkers van het VUmc kunnen bijdragen aan de uitvoering van een goed extern privacybeleid.

Uit de interviews blijkt dat het van belang is om voldoende awareness te bewerkstellingen onder werknemers en werknemers goed te informeren over de nieuwe wetgeving.¹⁹⁶

¹⁸⁸ Zie interview 7, bijlage V, p. 109

¹⁸⁹ Zie interview 1, bijlage V, p. 62, interview 3, bijlage V, p. 80

¹⁹⁰ Zie interview 3, bijlage V, p. 80

¹⁹¹ Zie interview 1, bijlage V, p. 62

¹⁹² Zie interview 4, bijlage V, p. 87, interview 8, bijlage V, p. 115

¹⁹³ Zie interview 4, bijlage V, p. 87

¹⁹⁴ Zie interview 8, bijlage V, p. 114

¹⁹⁵ Zie interview 2, bijlage V, p. 70, interview 8, bijlage V, p. 114-115

¹⁹⁶ Zie interview 1, bijlage V, p. 63, interview 3, bijlage V, p. 80, interview 4, bijlage V, p. 87, Zie interview 6, bijlage V, p. 104, interview 8, bijlage V, p. 116

Medewerkers hebben namelijk een hele belangrijke rol in de uitvoering van het extern privacybeleid. Zij moeten uitvoering geven aan het beleid en kunnen uitleggen hoe het beleid wordt gehanteerd.¹⁹⁷ Het grootste risico zit in onzorgvuldigheid en onwetendheid van de werknemers van werknemers. Om dat risico te beheersen heeft het VUmc e-learningmodules opgezet die alle medewerkers verplicht zijn te doen en eens in de twee jaar te herhalen, om zo te zorgen dat ze voldoende kennis behouden. Hierdoor kunnen medewerkers patiënten netjes informeren over wat zij weten over privacybescherming. Daarnaast heeft men binnen het VUmc een keer in de drie maanden contactpersonenoverleg Privacybescherming en Informatiebeveiliging. Iedere afdeling heeft een contactpersoon Privacybescherming en Informatiebeveiliging, zij krijgen tijdens een dergelijk overleg de nieuwste ontwikkelingen van de afdeling Privacybescherming en Informatiebeveiliging te horen en te zien. Het is dan de bedoeling dat deze contactpersonen de informatie meenemen naar hun afdeling. Ook hangt de afdeling Privacybescherming en Informatiebeveiliging posters op. Er wordt dus alles aan gedaan om zoveel mogelijk awareness te bewerkstelligen onder werknemers. Met die awareness zijn die medewerkers naar de patiënten toe adequater. Volgens de privacyportefeuillehouder en de medewerker van de Servicebalie hebben met name de baliemedewerkers een hele grote verantwoordelijkheid in de voorlichting van patiënten over privacy.¹⁹⁸ De baliemedewerkers zouden bijvoorbeeld een awarenessstraining moeten krijgen aangezien zij het visitekaartje van het VUmc zijn. Ze hebben niet alleen een passieve rol in het netjes opvolgen van het privacybeleid, maar ze hebben ook een actieve rol in de voorlichting van patiënten hierover. De privacyportefeuillehouder is daarnaast van mening dat ook artsen en andere medici een training moeten gaan volgen op het gebied van de AVG aangezien zij volgens haar niet bewust zijn van een heleboel zaken.¹⁹⁹ De stafadviseur Privacybescherming en Informatiebeveiliging is echter van mening dat hulpverleners zich net anders hoeven te gedragen aangezien zij vanuit de WGBO al verplicht zijn om patiënten te informeren over privacy. Dit dient vanuit de AVG alleen opnieuw benadrukt te worden.²⁰⁰

Dienst Communicatie zou kunnen bijdragen aan een goed extern privacybeleid door middel van de vertaling van het beleid naar wat het heel concreet betekent voor patiënten. Patiënten moeten hiervan op de hoogte zijn. Dienst Communicatie moet het beleid op zo'n manier aanbieden dat het in ieder geval de patiënten die er meer kennis van willen hebben de kans biedt om er daadwerkelijk meer van te weten te komen. De voornaamste rol van de Dienst Communicatie is het privacybeleid op het juiste moment, op de juiste manier aanbieden.²⁰¹

Het EVA Servicecentrum kan bijdragen aan een goed extern privacybeleid door vanuit de informatiemanagement zorg de ontwikkelingen in de gaten te houden en na te vragen om te beoordelen of bepaalde gegevensverstrekking wel past binnen de regels. Wanneer een

¹⁹⁷ Zie interview 6, bijlage V, p. 104

¹⁹⁸ Zie interview 4, bijlage V, p. 87, interview 8, bijlage V, p. 116

¹⁹⁹ Zie interview 4, bijlage V, p. 87

²⁰⁰ Zie interview 3, bijlage V, p. 80

²⁰¹ Zie interview 7, bijlage V, p. 109

bepaalde ontwikkeling nog niet bij de Functionaris Gegevensbescherming is geweest kunnen zij hem tippen dat er iets speelt.

Uit de antwoorden van de participanten blijkt dus dat de uitvoering van het intern privacybeleid eerst goed op orde dient te zijn, wil dit kunnen uitwerken in een goed extern privacybeleid.²⁰²

5.4.2 Toezicht

Wanneer het nieuwe extern privacybeleid na 25 mei 2018 ingaat, is het van belang om duidelijk te hebben wie er toezicht op gaat houden dat het beleid goed wordt nageleefd en dat patiënten daadwerkelijk voldoende geïnformeerd worden. Zoals we eerder zagen, stelt de AVG verplicht dat de Functionaris Gegevensbescherming toezicht houdt op de naleving van het extern privacybeleid. Het VUmc is echter een grote organisatie en de Functionaris Gegevensbescherming kan niet op heel gedetailleerd niveau toezicht houden. Aan de participanten van de afdeling Privacybescherming en Informatiebeveiliging is daarom gevraagd wie er op alle niveaus toezicht gaat houden op de naleving van het nieuwe extern privacybeleid.

Uit de interviews blijkt dat de Functionaris Gegevensbescherming, samen met de andere medewerkers van de afdeling Privacybescherming en Informatiebeveiliging in eerste instantie toezicht houdt op de naleving van het extern privacybeleid.²⁰³ Binnen deze afdeling bestaat er ook een PCDA-cyclus voor, er worden dus interne audits gedaan. Ook als er privacyincidenten of privacylekken zijn kijkt deze afdeling naar de oorzaken, waarna ze zorgen voor verbetermaatregelen. De toezicht en naleving op echt privacy-security stukken zit dus bij de afdeling Privacybescherming en Informatiebeveiliging.²⁰⁴ Daarnaast zijn op alle afdelingen de afdelingshoofden verantwoordelijk voor het handelen van de werknemers die onder hen functioneren.²⁰⁵ Wanneer het bijvoorbeeld gaat om een patiënt die een recht uitoefent en het VUmc heeft het niet of niet op tijd opgevolgd, is het afhankelijk van de verantwoordelijke voor dat proces. Inzage wordt bijvoorbeeld gegeven door afdeling Zorgetsteun en verwijdering van een dossier door de beheerders van het EPD. Het is dus afhankelijk van waar het is mis gegaan, wie daar ook verantwoordelijk voor is. In principes is naleving dus belegt bij diegene die verantwoordelijk is voor het proces. De afdeling Privacybescherming en Informatiebeveiliging kijkt organisatie breed. Wanneer zij iets horen gaan zij kijken waar het is misgegaan. Soms gaan zij gericht afdelingen auditen.²⁰⁶

²⁰² Zie interview 1, bijlage V, p. 63

²⁰³ Zie interview 1, bijlage V, p. 63, interview 2, bijlage V, p. 70-71

²⁰⁴ Zie interview 3, bijlage V, p. 80-81

²⁰⁵ Zie interview 1, bijlage V, p. 63, interview 3, bijlage V, p. 80-81

²⁰⁶ Zie interview 3, bijlage V, p. 80-81

Hoofdstuk 6: Conclusies en aanbevelingen

In de vorige hoofdstukken zijn door middel van literatuuronderzoek, analyse van wet- en regelgeving en interviews de deelvragen van dit onderzoek behandeld. In dit hoofdstuk zullen er naar aanleiding van het uitgevoerde literatuur- en praktijkonderzoek allereerst conclusies worden getrokken. Aan de hand van die bevindingen zal vervolgens antwoord worden gegeven op de centrale vraag: *‘Welk advies kan aan de hand van afgenomen interviews, analyse van wet- en regelgeving en literatuuronderzoek aan het VUmc worden gegeven over de inrichting van het extern privacybeleid en de praktische uitvoering daarvan, om voor 25 mei 2018 te voldoen aan de Algemene Verordening Gegevensbescherming?’*

6.1 Conclusies

Uit het literatuuronderzoek blijkt dat er onder de AVG strengere verplichtingen gaan gelden voor organisaties. De belangrijkste verplichting is dat organisaties kunnen aantonen dat zij daadwerkelijk aan de AVG voldoen. Dit wordt de verantwoordingsplicht genoemd. Dit betekent dus dat het VUmc aan haar patiënten moet kunnen aantonen dat zij goed met persoonsgegevens omgaat. Uit het literatuuronderzoek blijkt dat dit dient te worden aangetoond door middel van een extern privacybeleid. De AVG stelt de eis dat het extern privacybeleid op een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal verstrekt wordt.

Huidig extern privacybeleid

Uit de afgenomen interviews blijkt dat het huidige extern privacybeleid van het VUmc niet voldoet aan de AVG. Het is namelijk niet duidelijk wat het huidige extern privacybeleid van het VUmc inhoudt. Volgens de participanten staat er ‘iets’ op de website en bestaat er een folder met veel tekst, maar is er geen privacystatement op de website te vinden en is de folder niet gebaseerd op privacywetgeving, maar op de WGBO. Bovendien is deze folder niet op alle afdelingen te vinden. Daarnaast is het voor de meeste patiënten wel duidelijk dat zij met hun vragen terecht kunnen bij de Servicebalie, maar is het voor hen niet duidelijk dat zij zich ook rechtstreeks tot de Functionaris Gegevensbescherming mogen wenden. Dit wordt nergens vermeldt.

Inhoud extern privacybeleid

Uit het literatuuronderzoek blijkt dat de AVG precies heeft voorgeschreven welke onderwerpen het extern privacybeleid moet bevatten. Uit de interviews bleek dat de participanten goed op de hoogte waren van de eisen die de AVG stelt aan de inhoud van het extern privacybeleid. Op de vraag welke onderwerpen er in het extern privacybeleid van het VUmc moeten komen, benoemden zij dezelfde onderwerpen die de AVG noemt:

1. De identiteit en de contactgegevens van het VUmc;
2. de contactgegevens van de Functionaris Gegevensbescherming;

3. de doeleinden van en de rechtsgrond van de verwerking van de persoonsgegevens;
4. de gerechtvaardigde belangen van het VUmc, indien de verwerking op het gerechtvaardigd belang is gebaseerd;
5. de ontvangers of categorieën van ontvangers van de persoonsgegevens;
6. of de persoonsgegevens (zullen) worden doorgestuurd aan een derde land buiten de EU.
7. De bewaartermijn van de persoonsgegevens, of indien dat niet mogelijk is, de criteria ter bepaling van het bewaartermijn;
8. welke rechten de patiënt heeft;
9. dat de patiënt het recht heeft de toestemming te allen tijde in te trekken, zonder dat dit afbreuk doet aan de rechtmatigheid van de verwerking;
10. dat de patiënt het recht heeft een klacht in te dienen bij de toezichthouder;
11. of de verstrekking van persoonsgegevens een wettelijke of contractuele verplichting is dan wel een noodzakelijke voorwaarde om een overeenkomst te sluiten, en of de patiënt verplicht is de persoonsgegevens te verstrekken en wat de mogelijke gevolgen zijn wanneer deze gegevens niet worden verstrekt;
12. of het VUmc gebruik maakt van geautomatiseerde besluitvorming, de reden waarom zij dit doet, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

Het VUmc is dus verplicht deze onderwerpen in het extern privacybeleid op te nemen en uit te werken.

Communicatiekanalen extern privacybeleid

Uit het literatuuronderzoek blijkt dat de AVG verplicht dat het extern privacybeleid in gemakkelijk toegankelijke vorm verstrekt wordt. Dit betekent dus dat patiënten van het VUmc de informatie niet op moeten hoeven zoeken, maar dat het voor hen direct duidelijk moet zijn waar zij deze informatie kunnen vinden. Uit literatuuronderzoek blijkt dat het daarom van belang is om het extern privacybeleid via verscheidene communicatiekanalen aan patiënten bekend te maken. Werkgroep 29 heeft hier verschillende voorbeelden van gegeven. Uit de antwoorden van de participanten blijkt dat de belangrijkste communicatiekanalen om het extern privacybeleid aan patiënten van het VUmc bekend te maken zijn door middel van een privacystatement op de website van het VUmc, door middel van folders en patiëntenbrieven, via My Chart, via Narrow Casting en via de zorgovereenkomst.

Extern privacybeleid - Privacystatement

Uit het literatuuronderzoek blijkt dat het extern privacybeleid onder meer moet worden vertaald in een privacystatement op de website van het VUmc. De AVG verplicht dat het statement op een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal verstrekt wordt. Werkgroep 29 geeft het advies een gelaagd privacystatement op te stellen en daarbij gebruik te maken van aanvullende visualisatie.

Uit praktijkonderzoek blijkt dat het VUmc op dit moment geen duidelijk privacystatement heeft op haar website.

Inrichting

77,8 procent van de participanten was met Werkgroep 29 van mening dat er gebruik gemaakt moet worden van een gelaagd privacystatement. De volgende opties werden hierbij genoemd:

- Een kort privacystatement in begrijpelijke taal met daarin de mogelijkheid om door te klikken naar het externe privacybeleid, wat dan wat uitgebreider en juridisch complexer is.
- Een privacystatement met linkjes met verwijzingen naar achterliggende informatie.
- Een filmpje met de mogelijkheid om door te klikken naar achterliggende informatie.
- Een privacystatement met een verwijzing naar het register, naar reglementen en naar een toelichting door de FG.

Vormgeving en taalgebruik

Alle participanten waren tevens van mening het statement in zeer eenvoudige taal dient te worden opgesteld. Ook blijkt uit de interviews dat het van belang is om het privacystatement in het Nederlands, Engels en in een aantal andere gangbare talen op te stellen. Alle participanten waren daarnaast van mening dat er voor het privacystatement gebruik dient te worden gemaakt van aanvullende visualisatie. De belangrijkste zaken die hierbij genoemd werden waren het gebruik van een filmpje, of een stuk tekst met icoontjes of afbeeldingen.

Plaats op de website

Over de manier waarop het privacystatement op de website bekend moet worden gemaakt, kwamen er uit de interviews verscheidene opties naar voren. Slechts 22,2 procent van de participanten was van mening dat het privacystatement in de beginperiode heel duidelijk op de website dient te komen. 44,4 procent van de participanten vond dit niet nodig. Alle participanten waren echter wel van mening dat het statement makkelijk te vinden moet zijn op de website. Opties die hierbij genoemd werden waren het gebruik van een link, het plaatsen van het privacystatement onder het kopje 'Patiënteninformatie', onderaan het balkje op de website, onder het kopje 'Rechten en plichten' en bij het statement over cookies.

Extern privacybeleid - Folders

Uit de richtlijn van Werkgroep 29 blijkt dat het extern privacybeleid ook vertaald dient te worden in folders. Uit praktijkonderzoek blijkt dat de huidige folder of brochure gebaseerd is op de WGBO en dus niet voldoet aan de regelgeving van de AVG. Daarnaast blijkt dat niet bekend is of de huidige folder op alle afdelingen te vinden is. Hoewel de meningen over het belang van een folder verschilden, waren alle participanten wel van mening dat er een nieuwe folder moet komen conform de AVG. De twee opties die hierbij genoemd werden waren het opnemen van het volledige privacystatement in de folder of juist het slechts verwerken

van korte en bondige informatie met een verwijzing naar de website voor het privacystatement, meer verdieping en de contactgegevens van de Functionaris Gegevensbescherming. Uit de interviews blijkt ook dat het van belang is dat de folder verlevendigd wordt door middel van het gebruik van afbeeldingen. Tevens werd benoemd dat het van belang is dat deze nieuwe folder op alle afdelingen in de wachtkamers staan.

Uitvoering en toezicht extern privacybeleid

Zoals eerder naar voren kwam vloeit het opstellen van een extern privacybeleid voort uit de verantwoordingsplicht. Uit literatuuronderzoek blijkt echter dat niet alleen het opstellen, maar ook het op een juiste wijze uitvoeren van een extern privacybeleid van belang is om te voldoen aan de verantwoordingsplicht. Het is dus van belang dat het VUmc ook waar maakt wat er in het extern privacybeleid wordt gezegd en dus dat het VUmc ook het interne privacybeleid op orde heeft.

Werknemers

Uit praktijkonderzoek blijkt dat het VUmc inmiddels een intern privacybeleid heeft opgesteld. Daarnaast worden werknemers op diverse wijzen geïnformeerd en geïnstrueerd over de komst van de AVG en welke veranderingen dit met zich meebrengt. Uit de interviews blijkt dat het voornamelijk van belang is om onder baliemedewerkers awareness te bewerkstelligen, aangezien zij een belangrijke positie hebben in de voorlichting van patiënten.

Toezicht

Uit literatuuronderzoek blijkt dat de Functionaris Gegevensbescherming verantwoordelijk is voor toezicht op de naleving van het privacybeleid. Uit interviews blijkt echter dat deze taak voor de Functionaris Gegevensbescherming van het VUmc te groot is, aangezien de organisatie te groot is om op alle medewerkers toezicht te kunnen houden. Daarom hebben alle afdelingshoofden de verantwoordelijkheid over hun afdeling en houdt de afdeling Privacybescherming en Informatiebeveiliging organisatie breed toezicht.

6.2 Aanbevelingen

Aan de hand van de getrokken conclusies in de vorige paragraaf, zullen in deze paragraaf concrete aanbevelingen worden gedaan met betrekking tot de inrichting en uitvoering van het extern privacybeleid van het VUmc.

Huidig extern privacybeleid

Aangezien het VUmc op dit moment geen eenduidig extern privacybeleid hanteert, wordt er aanbevolen om alle huidige losse informatie in te trekken en een volledig nieuw extern privacybeleid op te stellen conform de regelgeving van de AVG.

Inhoud extern privacybeleid

Er wordt aanbevolen om een document op te stellen met de titel 'Extern privacybeleid'. In dit document dienen alle onderwerpen die besproken zijn in paragraaf 4.4 aan bod te komen. Er wordt aanbevolen om deze onderwerpen zodanig uit te werken dat het voor iedere patiënt

duidelijk is waar het over gaat, maar ook dat zij alle relevante informatie met betrekking tot het stellen van vragen hierin kan vinden. Dit document moet dus eenvoudig in taalgebruik zijn, maar hoeft niet direct heel beknopt te zijn.

Communicatiekanalen extern privacybeleid

Er wordt aanbevolen om diverse communicatiekanalen te gebruiken om het nieuwe extern privacybeleid te presenteren aan patiënten. Hierbij kan gebruikt gemaakt worden van een privacystatement op de website, een folder, informatie in patiëntenbrieven, een link naar het privacystatement in My Chart, informatie via Narrow Casting en informatie in de zorgovereenkomst. Er wordt aanbevolen om via deze communicatiekanalen niet het gehele extern privacybeleid aan te bieden maar deze in een beknopte, eenvoudige samenvatting met een verwijzing naar het volledige extern privacybeleid te presenteren.

Extern privacybeleid - Privacystatement

Er wordt aanbevolen om het extern privacybeleid te vertalen in een beknopt privacystatement op de website van het VUmc.

Inrichting

Wat betreft de inrichting van het privacystatement wordt aanbevolen om een gelaagd privacystatement op te stellen. De eerste laag van het statement moet dan een eenvoudig stuk tekst of een filmpje zijn met daarnaast de mogelijkheid om door te klikken naar uitgebreidere informatie en daarachter een verwijzing naar het volledige extern privacybeleid.

Vormgeving en taalgebruik

De vormgeving van het privacystatement en het taalgebruik in het privacystatement is van groot belang. Om alle patiënten te kunnen bereiken wordt er allereerst aanbevolen om het privacystatement minimaal in het Nederlands en in het Engels aan te bieden. Daarnaast wordt aanbevolen om bij de eerste laag van het statement gebruik te maken van een filmpje waarin alle onderwerpen kort en op zeer eenvoudige wijze worden uitgelegd, of gebruik te maken van een pagina op de website waarin alle onderwerpen middels korte teksten zeer eenvoudig worden uitgelegd. Hierbij wordt aanbevolen om gebruik te maken van ondersteunende afbeeldingen of matrixen. Daarnaast wordt er aanbevolen om bij de tweede laag van het statement de korte en bondige informatie uit de eerste laag nader uit te leggen. Dit kan bijvoorbeeld middels Q&A's. Deze achterliggende informatie dient nog steeds eenvoudig te zijn, maar mag wel meer tekst bevatten. Tot slot wordt aanbevolen om in de eerste en tweede laag te verwijzen naar het volledige extern privacybeleid.

Plaats op de website

Ook de plaats waar het privacystatement op de website wordt geplaatst is van groot belang. Er wordt aanbevolen om ervoor te zorgen dat de eerste laag van het privacystatement altijd direct te vinden is wanneer een patiënt zich op de website van het VUmc bevindt. Van belang is dus dat het statement via verschillende wegen te vinden is. Allereerst wordt aanbevolen om onderaan de website een kopje 'Privacystatement' te plaatsen, waarachter direct het

statement zelf met de daarbij horende verwijzingen te vinden is. Daarnaast wordt aanbevolen om het privacystatement onder het kopje 'Patiënteninformatie' te plaatsen op de homepage van de website. Tot slot wordt aanbevolen om een link met een verwijzing naar het privacystatement te zetten bij het statement over cookies.

Extern privacybeleid – Folder

Naast het gebruik van een privacystatement wordt tevens aanbevolen het extern privacybeleid te vertalen naar een folder. Er wordt aanbevolen deze folder op een aantrekkelijke wijze vorm te geven door middel van het gebruik van in het oog springende afbeeldingen. Wat betreft de inhoud van de folder wordt er aanbevolen om op een zeer beknopte en eenvoudige wijze alle onderwerpen uit het extern privacybeleid te bespreken, met daarnaast een verwijzing naar het privacystatement op de website en het volledige extern privacybeleid. Ook wordt aanbevolen om duidelijk aan te geven wie de Functionaris Gegevensbescherming is en aan te geven waar patiënten terecht kunnen met hun vragen met betrekking het privacybeleid.

Uitvoering en toezicht extern privacybeleid

Werknemers

Hoewel het VUmc al een intern privacybeleid heeft opgesteld en op actieve wijze haar werknemers aan het voorlichten is over dit beleid, wordt aanbevolen om ook voldoende awareness te bewerkstelligen wat betreft het extern privacybeleid. Werknemers moeten niet alleen weten hoe zij op een zorgvuldige wijze om dienen te gaan met persoonsgegevens, maar moeten ook weten hoe zij vragen van patiënten over het privacybeleid dienen te beantwoorden. Aanbevolen wordt dus om werknemers een awarenessstraining te geven met betrekking tot het extern privacybeleid. Er wordt met name aanbevolen om de baliemedewerkers, servicemedewerkers en klachtenfunctionarissen periodiek te trainen zodat zij altijd in staat zijn om patiënten te woord te staan op dit gebied, en het VUmc hierdoor aan de transparantieplicht en de verantwoordingplicht voldoet.

Toezicht

De toezicht op het intern privacybeleid van het VUmc is op dit moment op orde. Aanbevolen wordt om met de komst van het extern privacybeleid binnen de organisatie een goede taakverdeling te maken wat betreft de toezicht hierop. Er wordt aanbevolen om met name toezicht te houden op baliemedewerkers, servicemedewerkers en klachtenfunctionarissen, om in de gaten te houden of zij patiënten voldoende kunnen informeren met betrekking tot privacy en de verwerking van persoonsgegevens.

Behaald resultaat

Het doel van dit onderzoek was om op 26 april 2018 bij de heer Marcel van der Haagen, Functionaris Gegevensbescherming van het VUmc, een rapport in te leveren, waarin op basis van afgenomen interviews, analyse van wet- en regelgeving en literatuuronderzoek conclusies zijn getrokken en aanbevelingen worden gedaan over de wijze waarop het VUmc het extern privacybeleid moet inrichten en uitvoeren zodat het voldoet aan de Algemene Verordening Gegevensbescherming en hierdoor de privacyrechten van de patiënten van VUmc het beste worden gewaarborgd.

Aangezien uit het literatuuronderzoek en het praktijkonderzoek concrete conclusies konden worden getrokken en concrete aanbevelingen konden worden gedaan, waarmee het VUmc op 26 april 2018 duidelijke handvatten heeft gekregen om een extern privacybeleid conform de AVG op te stellen en uit te voeren, kan er worden gezegd dat het beoogde resultaat is behaald. Daarnaast heeft de opdrachtgever aangegeven dat op basis van de inhoud, opbouw en schrijfstijl onderdelen van dit rapport heel goed kunnen worden gebruikt als leerstof voor Functionarissen Gegevensbescherming.

Literatuurlijst

Literatuur

Arts, Privacycompany.eu augustus 2017

C. Arts, 'Hoe geef je invulling aan de verschillende rechten van betrokkenen: het recht van bezwaar', *Privacycompany.eu* 14 augustus 2017

Arts, Privacycompany.eu september 2017

C. Arts, 'Hoe geef je invulling aan de verschillende rechten van betrokkenen: het recht op beperking van de verwerking', *Privacycompany.eu* 5 september 2017.

Van Balen en Nijveld, Tijdschrift voor Gezondheidsrecht 2018, afl. 8, p. 608

Van Balen en Nijveld, 'De Algemene verordening gegevensbescherming: een introductie voor de zorgsector', *Tijdschrift voor Gezondheidsrecht* 2018, afl. 8, p. 608

Binnema & J. Frederiksz, europadecentraal.nl maart 2018

M. Binnema & J. Frederiksz, 'AVG Deel III: Verwerker, verwerkingsverantwoordelijke en verwerkersovereenkomst', *europadecentraal.nl*, 5 maart 2018

Bouma, NRC april 2018

F. Bouma, '85 medewerkers Hagaziekenhuis berispt na inbreuk dossier Barbie', *NRC* 26 april 2018

Engelfried, Emerce.nl februari 2018

A. Engelfried, 'AVG compliance: het verwerkingsregister – vastleggen wat u doet met persoonsgegevens', *emerce.nl* 18 februari 2018

Ephimenco, de Trouw 7 april 2018

S. Ephimenco, 'Wie om privacy geeft, moet vooral Facebook schreeuwend ontvluchten', *Trouw* 7 april 2018.

Van Essen, solv.nl juni 2016

T. van Essen, 'Het toepassingsgebied van de AVG', *solv.nl* 27 juni 2016

Huissen 2015

R. Huissen, 'Privacy in de zorg' 'Van wie is uw medisch dossier?', Amsterdam: Uitgeverij SWP 2015

Van der Jagt, in: Grondrechten 2013

F.C. van der Jagt, 'Het recht op bescherming van persoonsgegevens', in: J.H. Gerards e.a. (red.) *Grondrechten. De nationale, Europese en internationale dimensie*, Nijmegen: Ars Aequi Libri 2013

Leenen e.a. 2017

H.J.J. Leenen, J.C.J. Dute, J.K.M. Gevers, J. Legemaate, G.R.J. de Groot, M.E. Gelpke, E.J.C. de Jong, *Handboek gezondheidsrecht*, Den Haag: Boom Juridisch 2017

Matto, Baalbergen & Marouf

Matto, Baalbergen & Marouf, *De Algemene verordening gegevensbescherming en de gevolgen voor organisaties. Voor een duurzame digitale samenleving (white paper)*, *advisor.nl*, p. 1-3

Stephanian, tenholdernoordam.nl december 2017

M. Stephanian, 'AVG Uitgediept #11: Wel of geen Data Protection Impact Assessment?' *tenholternoordam.nl* 5 december 2017

Visser, Privacycompany.eu augustus 2017

A. Visser, 'Hoe geef je invulling aan de verschillende rechten van betrokkenen: geautomatiseerde besluiten en profiling', *Privacycompany.eu* 7 augustus 2017

De Vries en Goudsmit, Nederlands Juristenblad 2016/1077, afl. 22

H. de Vries & M. Goudsmit, 'Voorsorteren op de Algemene Verordening Gegevensbescherming. Twee stappen vooruit, één stap terug.', *Nederlands Juristenblad* 2016/1077, afl. 22

Wijnant, ictrecht.nl januari 2017

M. Wijnant, 'Artikel 29-werkgroep publiceert richtlijnen voor begrippen van de Europese privacywet', *ictrecht.nl*, 2 januari 2017

Van der Zwan, Linkedin.com september 2016

K. Van der Zwan, 'PRIVACYBELEID: wat staat daar in?', *Linkedin.com*, 12 september 2016
<https://nl.linkedin.com/pulse/privacybeleid-wat-staat-daar-kirsten-van-der-zwan>

Parlementaire stukken en richtlijnen

Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 17/EN, WP 248 rev.01

Guidelines on Data Protection Officers ('DPOs'), 16/ EN, WP243

Guidelines on transparency under Regulation 2016/679, 17/ EN, WP260

Kamerstukken II 2017/18, 34851, 3, p. 45 (MvT)

Ministerie van Volksgezondheid, Welzijn en Sport 2017

Ministerie van Volksgezondheid, Welzijn en Sport, *Elektronische gegevensuitwisseling in de zorg*, juni 2017 (brochure)

Overig

Autoriteit persoonsgegevens

1. 'Algemene informatie AVG', *autoriteitpersoonsgegevens.nl*, geraadpleegd op: 8 februari 2018
<https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/algemene-informatie-avg>
2. 'Algemene informatie AVG' onder het kopje 'Algemene vragen over de AVG, 'Wat zijn de belangrijkste veranderingen voor organisaties?', *autoriteitpersoonsgegevens.nl*, geraadpleegd op: 12 maart 2018
<https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/algemene-informatie-avg>
3. 'Zorgverleners en de AVG', *autoriteitpersoonsgegevens.nl*, geraadpleegd op: 22 februari 2018
<https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/gezondheid/zorgverleners-en-de-avg>
4. 'Data protection impact assessment (DPIA)', *autoriteitpersoonsgegevens.nl*, geraadpleegd op: 8 februari 2018
<https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/data-protection-impact-assessment-dpia>
5. 'European Data Protection Board vandaag van start', *autoriteitpersoonsgegevens.nl*, geraadpleegd op: 26 mei 2018
<https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/european-data-protection-board-vandaag-van-start>

6. 'Internationale privacywetgeving', *autoriteitpersoonsgegevens.nl*, geraadpleegd op: 19 februari 2018
<https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/internationale-privacywetgeving>
7. 'In 10 stappen voorbereid op de AVG', *Autoriteitpersoonsgegevens.nl*, gedownload op: 9 februari 2018
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/in_10_stappen_voorbereid_op_de_avg.pdf
8. 'Mag u persoonsgegevens verwerken?' onder het kopje 'Vragen over grondslagen', 'Wanneer mag u zich baseren op de grondslag gerechtvaardigd belang?' *autoriteitpersoonsgegevens.nl*, geraadpleegd op: 16 maart 2018
<https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/mag-u-persoonsgegevens-verwerken>
9. 'Mag u persoonsgegevens verwerken?' onder het kopje 'Vragen over grondslagen', 'Wanneer mag u zich baseren op de grondslag uitvoering overeenkomst?' *autoriteitpersoonsgegevens.nl*, geraadpleegd op: 15 maart 2018
<https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/mag-u-persoonsgegevens-verwerken>
10. 'Mag u persoonsgegevens verwerken?' onder het kopje 'Vragen over grondslagen', 'Wanneer mag u zich baseren op de grondslag wettelijke verplichting?', *autoriteitpersoonsgegevens.nl*, geraadpleegd op: 16 maart 2018
<https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/mag-u-persoonsgegevens-verwerken>
11. 'Mag u persoonsgegevens verwerken?' onder het kopje 'Vragen over persoonsgegevens verwerken', 'Hoe weet u of u persoonsgegevens mag verwerken?' *autoriteitpersoonsgegevens.nl*, geraadpleegd op: 12 maart 2018
<https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/mag-u-persoonsgegevens-verwerken>
12. 'Privacy by Design' *autoriteitpersoonsgegevens.nl*, geraadpleegd op: 19 maart 2018
<https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacycheck/privacy-design>

13. 'Rechten van betrokkenen' onder het kopje 'Vragen over het recht op dataportabiliteit', *autoriteitpersoonsgegevens.nl*, geraadpleegd op: 8 februari 2018
<https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/rechten-van-betrokkenen>
14. 'Verantwoordingsplicht', *autoriteitpersoonsgegevens.nl*, geraadpleegd op: 12 maart 2018
<https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/verantwoordingsplicht>
15. 'Wat zijn persoonsgegevens?' onder het kopje 'Wie is de verwerkingsverantwoordelijke en wie is de betrokkene bij het verwerken van persoonsgegevens?'
autoriteitpersoonsgegevens.nl, geraadpleegd op: 11 april 2018
<https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/wat-zijn-persoonsgegevens>
16. 'Wetten' onder het kopje 'Wet bescherming persoonsgegevens',
autoriteitpersoonsgegevens.nl, geraadpleegd op: 6 februari 2018
<https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten>

Europadecentraal.nl

'Register van verwerkingsactiviteiten', *europadecentraal.nl*, geraadpleegd op: 20 maart 2018
<https://europadecentraal.nl/onderwerp/informatiemaatschappij/gegevensbescherming-en-de-avg/verplichtingen-verantwoordelijke/register-van-de-verwerkingsactiviteiten/>

Europa-nu.nl

'Bescherming van persoonsgegevens in Europa', *europa-nu.nl*, geraadpleegd op: 8 februari 2018
https://www.europa-nu.nl/id/vhkejco8liwc/bescherming_van_persoonsgegevens_in

Nederlandict.nl maart 2017

'De Avg uitgelegd deel 2: transparantie en het recht op informatie', 8 maart 2017,
Nederlandict.nl, geraadpleegd op: 12 maart 2018
<https://www.nederlandict.nl/news/de-avg-uitgelegd-deel-2-transparantie-en-het-recht-op-informatie/>