Openheid van zaken

Een onderzoek naar de wijze waarop het toekomstige privacybeleid, toegespitst op de afdeling personeelszaken, van het UMCG, kan worden ingericht, zodat deze compliant is aan de bepalingen van de EPV.

Nicky Oolderink

Juridische Zaken
Hanzehogeschool, Rechten

Groningen, juni 2016

Studentenbureau UMCG

Universitair Medisch Centrum Groningen

Trefw Privacybeleid, privacyrecht, privacywetgeving, privacyregelement

Openheid van zaken

Een onderzoek naar de wijze waarop het toekomstige privacybeleid, toegespitst op de afdeling Personeelszaken, van het UMCG kan worden ingericht, zodat deze compliant is aan de bepalingen van de EPV

Groningen, juni 2016

Auteur	Nicky Oolderink
Studentnummer	310929
Afstudeerscriptie in het kader van	Privacyrecht Rechten Hanzehogeschool
Opdrachtgever	Mr. Robert Jager Juridische zaken, UMCG
Begeleider onderwijsinstelling	Mr. J. Wintjes Hanzehogeschool
Begeleider UMCG	B. Sieperda, FG Privacy Werkorganisatie, UMCG

Voorwoord

Voor u ligt het afstudeeronderzoek dat ik uit heb mogen voeren als afsluiting van de opleiding HBO-rechten. Tijdens deze opleiding heb ik veel kennis mogen opdoen met betrekking tot verschillende rechtsgebieden. Daarnaast heb ik, door het volgen van deze opleiding, de kans gekregen om praktijkervaring op te doen in de vorm van een stageperiode van vijf maanden op een advocatenkantoor te Curaçao.

Graag wil ik de personen die hebben bijgedragen aan de totstandkoming van mijn afstudeeronderzoek bedanken. Allereerst mijn praktijkbegeleider Boudien Sieperda. Zonder haar advies en tips had ik mijn afstudeeronderzoek niet op deze wijze kunnen afronden. Daarnaast wil ik mevrouw J. Zaal bedanken voor het delen van haar kennis met betrekking tot het doen van onderzoek en privacywetgeving. Tevens verdienen alle respondenten die hebben meegewerkt aan het praktijkonderzoek een bedankje. Zonder hen had ik mijn praktijkonderzoek niet naar behoren kunnen uitvoeren.

Daarnaast wil ik graag mijn afstudeerdocent Joey Wintjes bedanken voor haar advies en tips. Mede door haar energie heb ik dit onderzoek tijdig tot een goed einde weten te brengen. De laatste personen die ik wil bedanken zijn Marcel Oolderink, Wilma Oolderink, Maarten Oolderink, Ruben Oolderink en Sophie de Groot. Hun onvoorwaardelijke steun heeft ervoor gezorgd dat ik mijn studie met plezier kon volgen en afronden.

Ik wens u veel leesplezier toe!

Lijst met afkortingen

CBP	College Bescherming Persoonsgegevens
Wbp	Wet bescherming persoonsgegevens
AP	Autoriteit Persoonsgegevens
EPV	Europese Privacy Verordening
BW	Burgerlijk Wetboek
P&O	Personeelszaken
Wgbo	Wet op de geneeskundige behandelingsovereenkomst
MvT	Memorie van Toelichting
FG	Functionaris voor de Gegevensbescherming
WOR	Wet op de Ondernemingsraden
OR	Ondernemingsraad

Inhoudsopgave

1. Inleiding

1.1 Het onderzoekskader

1.1.1 De praktische aanleiding van het onderzoek

De praktische aanleiding van het onderzoek is de inwerkingtreding van de nieuwe Europese Privacy Verordening (EPV). De huidige nationale privacywetgeving is vastgelegd in de Wet Bescherming Persoonsgegevens (Wbp) uit 2000.[1] Deze wet is de uitkomst van het omzetten van de Europese privacyrichtlijn uit 1995 naar Nederlandse wetgeving. Het recht op privacy is een mensenrecht, welke opgenomen is in artikel 10 van de Grondwet, artikel 12 van de Universele verklaring van de rechten van de mens, artikel 16 van het Verdrag betreffende de werking van de Europese Unie en artikel 7 en 8 Handvest van de Grondrechten van de Europese Unie.[2]

De Europese privacyrichtlijn stamt uit een tijdperk waarin het internet net zijn opkomst maakte. De samenleving wordt in een hoog tempo overvallen door de nieuwe technologie. Informatie die eerst moeizaam uit papieren bronnen gehaald moest worden, is nu eenvoudig bereikbaar via het internet.[3] De technologie heeft zich sindsdien alleen maar verder ontwikkeld. Hierdoor zijn er uitdagingen met betrekking tot de bescherming van persoonsgegevens ontstaan. De overheid en bedrijven maken meer dan ooit gebruik van deze persoonsgegevens en natuurlijke personen maken hun persoonsgegevens veel vaker (onbewust) bekend door middel van wereldwijde netwerken.[4]

Daarnaast was de privacywetgeving niet uniform geregeld in Europa, waardoor er grote verschillen zaten in het omgaan met de persoonsgegevens tussen Europese landen. De Europese Commissie heeft om deze redenen een aantal jaren geleden besloten dat de Wbp aan herziening toe was. Deze herziening vindt zijn uitwerking in de EPV.[5]

Door het in werking treden van de EPV zullen er verschillende wijzigingen plaatsvinden in de huidige privacyregels. Deze zullen vastgelegd worden in een nieuwe verordening. Dit onderzoek is erop gericht om de gevolgen die de EPV met zich meebrengt, op het gebied van het hebben van een privacybeleid[6], in kaart te brengen voor het Universitair Medisch Centrum Groningen (UMCG). Het UMCG heeft, met haar vele medewerkers en patiënten, te maken met een grote hoeveelheid persoonsgegevens. Vaak zijn deze persoonsgegevens van vertrouwelijke en/of gevoelige aard. Door het invoeren van de EPV krijgt elke organisatie die met persoonsgegevens werkt de verplichting om een privacybeleid op te stellen en deze, met betrekking tot het verwerken van persoonsgegevens, te gebruiken in de organisatie.

Op dit moment bestaat het vermoeden dat er sprake is van een versnipperd privacybeleid in het UMCG. Niet overal is duidelijk wat er bestaat aan privacybeleid, wat de verschillen hierin per afdeling zijn, wat het eventuele ongeschreven beleid omvat en hoe de verschillende medewerkers hiermee omgaan. Het UMCG heeft het doel om op de korte termijn te zorgen voor een uniform privacybeleid, waarin het UMCG zich houdt aan de nieuwe regels uit de EPV en sancties door overtredingen, zoals boetes, vermeden worden.

Er is een verschil tussen (het opstellen van) beleid en de uitvoering daarvan. Dit onderzoek richt zich vooral op het inventariseren van het huidige beleid van het UMCG en het inventariseren van de EPV.

[1] Van der Wijst 2014.
[2] Steffin 2014, p. 36-37.
[3] Berkvens 2002, p. 2.
[4] Overweging 6 EPV.
[5] Van Oosterhout 2015.
[6] *Een privacybeleid is te definiëren als een (schriftelijk) geheel van gedragsregels met doelstellingen, waarin wordt beschreven hoe er in een organisatie met het verwerken van persoonsgegevens moet worden omgegaan.*

Daarnaast worden er aanbevelingen gedaan aan het UMCG voor het opstellen van het nieuwe privacybeleid. In dit onderzoek zal gekeken worden hoe het privacybeleid geformuleerd dient te worden, zodat een correcte uitvoering van het privacybeleid bereikt kan worden. Uiteindelijk is het namelijk tevens belangrijk hoe de uitvoering van het beleid plaatsvindt, omdat er zowel sancties kunnen volgen bij het niet hebben van het privacybeleid als bij het niet goed in uitvoering brengen daarvan. Er wordt echter geen apart onderzoek verricht naar de uitvoering van beleid. Hoe er op de werkvloer met bepaalde regels omgegaan en gecommuniceerd wordt, is namelijk weer een apart onderzoek. Onderzoek hiernaar doet afbreuk aan de diepte van het eigenlijke onderzoek.

1.1.2 Relevantie

Het UMCG verwerkt als ziekenhuis een groot aantal (vertrouwelijke) persoonsgegevens. Dit zijn de gegevens van zowel patiënten als medewerkers. Op dit moment is er, zoals eerder aangegeven in de praktische aanleiding van het onderzoek, niet volledig bekend wat er bestaat aan beleid en lijkt het beleid op het gebied van privacy versnipperd. De nieuwe privacyregelgeving kan leiden tot ingrijpende gevolgen voor de processen, procedures en systemen van het UMCG. Toezichthouders hebben met de inwerkingtreding van de EPV namelijk bevoegdheden gekregen die zij eerder niet hadden, namelijk het opleggen van zwaardere sancties indien een organisatie zich niet houdt aan de regelgeving. Ook is de EPV er mede op gericht dat organisaties privacybeleid als belangrijk onderwerp gaan zien. Door de strengere voorschriften dienen organisaties goed te overwegen hoe zij het beleid met betrekking tot privacy gaan vormgeven en of de uitvoerbaarheid hiervan haalbaar is. Indien het UMCG dit niet naar behoren doet, riskeert zij hoge boetes. Het is voor het UMCG daarom erg van belang om te weten welke wijzigingen precies zijn doorgevoerd in de privacywetgeving. Hierdoor zal het UMCG adequaat op de wetswijzigingen kunnen reageren door bijvoorbeeld haar privacybeleid aan te passen en de medewerkers hierover voor te lichten.

1.1.3 Actoren binnen het UMCG

De opdrachtgever van het onderzoek is de 'Privacy werkorganisatie' en het hoofd van Juridische Zaken. Het onderzoek is toegespitst op de afdeling Personeelszaken [P&O] van het UMCG. Daarom zijn ook de medewerkers van het UMCG belangrijke actoren in dit onderzoek. Enerzijds omdat de persoonsgegevens van deze betrokkenen worden verwerkt door het UMCG, aangezien er sprake is van het bijhouden van personeelsdossiers. Anderzijds omdat personeelsleden op de afdeling P&O met deze gegevens moeten omgaan en deze gegevens moeten verwerken. Op dit moment is er onder het personeel vermoedelijk nog onbekendheid over hoe precies aan privacy wet- en regelgeving moet worden voldaan, omdat een uniform beleid over het verwerken van deze gegevens ontbreekt. Met de inwerkingtreding van de EPV zal het hanteren van een dergelijk uniform beleid verplicht zijn, waardoor er veranderingen binnen het UMCG zullen plaatsvinden.

De Privacy werkorganisatie van het UMCG verdiept zich al langere tijd in de komst de EPV. Voor de komst van de Privacy werkorganisatie was er al een Functionaris voor de Gegevensbescherming (FG) aangesteld, die naast deze functie ook andere werkzaamheden had. Anticiperend op de komst van de EPV is er een tweede Functionaris voor de Gegevensbescherming aangesteld, die zich bezighoudt met het beschermen van persoonsgegevens. Op dat moment is ook de Privacy werkorganisatie opgericht die formeel is gepositioneerd onder Juridische Zaken. In de Privacy werkorganisatie zitten de twee Functionarissen voor de Gegevensbescherming, een Information Security Officer, een aantal juristen en ook nog een aantal communicatief opgeleide medewerkers.

1.1.4 Externe actoren

Jos van der Wijst, werkzaam bij Bogaerts & Groenen advocaten, geeft in zijn gepubliceerde artikel aan dat de veranderingen ten opzichte van de huidige regelgeving groot zijn en daarmee veel stof heeft doen opwaaien.[7] Van der Wijs beschrijft de veranderingen als volgt:

[7] Van der Wijst 2014.

'De organisatie krijgt de verplichting om, nog meer dan nu al het geval is, goed te documenteren. Nu geldt onder omstandigheden een meldplicht bij het CBP. Onder de verordening wordt het een verplichting voor bedrijven om het doel van de bewerking van persoonsgegevens te beschrijven en het proces correct in te richten. Iedere organisatie die met persoonsgegevens werkt krijgt nu de verplichting om een ***privacybeleid*** *te formuleren en daarin bepaalde aspecten op te nemen.'*

'Voor bedrijven die in meerdere Lid-Staten werken is dit goed nieuws. Nu hebben ze te maken met verschillende nationale toezichthouders die bevoegd zijn. Wanneer het voorstel wordt aangenomen krijgen deze bedrijven met ***één Europese toezichthouder*** *te maken. Voor de bedrijven die niet in meerdere Lid-Staten werken verandert er niets. Zij blijven te maken krijgen met hun nationale toezichthouder zoals in Nederland het College Bescherming Persoonsgegevens (CBP).'*

'De verordening introduceert het recht om vergeten te worden. Recent heeft het Europees Hof in een zaak tegen Google bepaald dat een natuurlijk persoon het recht heeft om te vragen zijn persoonsgegevens te verwijderen uit zoekresultaten. Een dergelijk recht wordt nu ook in de verordening vastgelegd. Dit betekent dat een organisatie persoonsgegevens moet verwijderen indien; er niet langer een noodzaak is om de gegevens te bewaren gelet op het doel waarvoor de gegevens verzameld zijn, de natuurlijk persoon zijn toestemming intrekt om de persoonsgegevens te bewaren, de natuurlijk persoon bezwaar maakt tegen het gebruiken van zijn persoonsgegevens, de organisatie de verordening niet naleeft.'

De Nederlandse Vereniging Ziekenhuizen [NVZ] heeft geanalyseerd welke ontwikkelingen met betrekking tot de nieuwe privacyregelgeving aandachtspunten zijn voor zorgaanbieders. Het NVZ heeft in kaart gebracht welke veranderingen zij verwacht:[8]
- 'Wie patiëntgegevens verwerkt moet een transparant en eenvoudig toegankelijk beleid hebben vastgesteld met betrekking tot de gegevensverwerking en de rechten van de betrokkenen;
- Gegevensbeschermingsbeleid moet worden geformuleerd voor de gehele levenscyclus van gegevensverwerking, vanaf het verzamelen tot en met het vernietigen van persoonsgegevens;
- Wie gevoelige persoonsgegevens verwerkt, zoals patiëntgegevens, moet de gegevensverwerking onderwerpen aan een 'privacyeffectbeoordeling';
een patiënt moet verzoeken inzake de uitoefening van zijn rechten desgewenst elektronisch kunnen indienen;
- Het College Bescherming Persoonsgegevens (CBP) krijgt de bevoegdheid om boetes op te leggen tot maximaal 100 miljoen euro of vijf procent van de jaaromzet van de organisatie. Aandacht verdient het feit dat het CBP sinds 1 januari 2016 een nieuwe naam heeft gekregen, namelijk de Autoriteit Persoonsgegevens (AP).'
- Daarnaast stelt de NVZ dat het instellen van een privacyfunctionaris, ofwel een Functionaris voor de Gegevensbescherming (FG), verplicht is voor een zorgaanbieder.[9] De EPV verplicht organisaties een privacyfunctionaris aan te stellen indien de kernactiviteiten van de voor de verwerking verantwoordelijke of de verwerker bestaan uit de verwerking van bijzondere categorieën gegevens ingevolge artikel 9, lid 1 EPV. Volgens het voorgenoemde artikel vallen gegevens met betrekking tot de gezondheid van patiënten onder deze bijzondere gegevens. Dit heeft als gevolg dat zorgaanbieders, zoals het UMCG, verplicht zijn een privacyfunctionaris in te stellen.

1.1.5 Belangrijke wet- en regelgeving

De praktische aanleiding van het onderzoek is de invoering van de EPV. Deze verordening zal de huidige wetgeving, de Wbp, gaan vervangen. De EPV en de Wbp, en dan vooral de verschillen en overeenkomsten tussen deze twee wetten, vormen dus de basis van dit onderzoek. In dit onderzoek wordt vooral toegespitst op het artikel in de EPV waarin een privacybeleid verplicht wordt gesteld.[10]

[8] NVZ 2014.
[9] NVZ 2014.
[10] Artikel 22 lid 1 EPV.

1.1.6 Eerder onderzoek

Er is eerder onderzoek verricht naar de werking van de Wbp. In artikel 80 van de Wbp is opgenomen dat er binnen vijf jaren na de inwerkingtreding van de Wbp een wetsevaluatie diende plaats te vinden. Dit houdt in dat binnen deze vijf jaren de Ministers van Justitie en van Binnenlandse zaken en Koninkrijksrelaties een verslag moesten doen aan de Staten-Generaal over de werking van de Wbp in de praktijk. Hierbij dienden eventuele knelpunten naar voren gebracht te worden. Belangrijk was of de Wbp de bescherming van de persoonsgegevens in de praktijk naar behoren waarborgde.

Bovenstaand onderzoek, verplicht door artikel 80 van de Wbp, werd uitgevoerd door het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) in de vorm van twee onderzoeksrapporten. Reden voor deze opsplitsing is dat de Wbp een zeer groot terrein bestrijkt. Het eerste onderzoeksrapport verscheen in 2007. Het WODC heeft dit (knelpunten)onderzoek verricht met behulp van relevante literatuur en rechtspraak. In de eerste fase van het onderzoek is het theoretische gedeelte van het totale onderzoek in kaart gebracht. De eerste fase kan worden opgedeeld in drie aparte delen. In het eerste deel van fase één is onderzocht wat de doelstellingen van de Gemeenschapswetgever waren bij het opstellen van de richtlijn. In het tweede deel werd onderzocht wat de doelstellingen van de nationale wetgever waren bij het implementeren van de richtlijn. Als laatste heeft er een knelpuntenanalyse plaatsgevonden. Hierbij werd gekeken welke knelpunten in de werking van de Wbp naar voren zijn gekomen in literatuur en jurisprudentie.[11]

De doelstellingen van de Europese wetgever die zijn voortgekomen in deel één van fase één worden hieronder vermeld. Allereerst moet de Wbp bijdragen aan de verwezenlijking van de algemene doelstellingen van de gemeenschap door een bijdrage te leveren aan de totstandbrenging en werking van de interne markt. Dit wilde de wetgever bereiken door marktbelemmeringen te voorkomen, die kunnen ontstaan doordat er verschil is in de privacywetgeving van diverse landen. De Wbp heeft daarom een ruime werking, gericht op geautomatiseerde verwerkingen, gekregen. Daarnaast dient de Wbp waarborgen te bieden voor de bescherming van fundamentele rechten en vrijheden. In de Wbp wordt daarom verwezen naar het EVRM en de privacybeginselen uit het Verdrag inzake gegevensbescherming. Tevens moest er sprake zijn van transparantie van gegevensverwerkingen. De wetgever wilde tevens dat de Wbp met oog op de verschillende branches en sectoren een flexibele manier van werken had. Hiervoor heeft de wetgever in de Wbp de mogelijkheid en ruimte gegeven dat er op branche- en sectorniveau gedragscodes worden opgesteld.[12]

In het tweede deel van fase één werden de doelstellingen van de nationale wetgever in kaart gebracht. Het WODC heeft dit onderdeel opgedeeld in twee soorten doelstellingen; formele doelstellingen en materiële doelstellingen. De formele doelstellingen zijn gericht op het feit dat de wetgever rekening dient te houden met hogere wetgeving. De materiële doelstellingen zien toe op de manier van bereiken van de formele doelstellingen. De eerste formele doelstelling van de nationale wetgever was dat de richtlijn geïmplementeerd moest worden in nationale wetgeving.[13] De tweede formele doelstelling is het inrichten van bepalingen met betrekking op het opslaan, verwerken en beschermen van persoonsgegevens. Tot slot dient het Verdrag inzake gegevensbescherming in uitvoer gebracht te worden en moet er rekening gehouden worden met de rechtspraak van het EHRM. De eerste materiële doelstelling van de nationale wetgever was dat er zowel privacybescherming als de rest van de grondrechten gewaarborgd zouden worden in de Wbp. Daarnaast vond de nationale wetgever het belangrijk dat er op een transparante manier met persoonsgegevens werd omgegaan door organisaties. Dit wilde de wetgever bereiken door rechten toe te kennen aan betrokkenen die hun persoonsgegevens verstrekken. Organisaties kregen hierop de verplichtingen om te handelen naar de rechten die deze betrokkenen hebben. Daarnaast was het belangrijk dat er een toezichthoudend orgaan werd ingesteld. De nationale wetgever heeft daarom

[11] WODC 1 2007, p. 16.
[12] WODC 1 2007, p. 9.
[13] WODC 1 2007, p. 9.

de Autoriteit Persoonsgegevens (AP) ingesteld en de vrijheid aan organisaties gegeven om een FG in te stellen. Hierdoor zouden organisaties zich bewuster met de verwerking en vastlegging van persoonsgegevens moeten gaan bezighouden.[14]

Naast bovengenoemde bevat fase één nog een laatste deel, de knelpunteninventarisatie. Hieronder worden de belangrijkste knelpunten weergegeven:
Uit het onderzoek bleek als eerste dat een aantal verschillende schrijvers onduidelijkheid en onbepaaldheid van de wettelijke begrippen als een knelpunt zien. Er waren ook weer schrijvers die de ruimte die hier wordt gelaten een goed initiatief vinden zodat er ruimte tot eigen invulling is. Daarnaast gaven verschillende schrijvers aan dat zij één privacywet voor alle sectoren en branches niet handig vinden. Dit wordt ook wel een omnibuskarakter genoemd. Eén auteur vond dit wel nodig, zodat er samenhang is tussen de belangen van alle verschillende partijen. Dit zou zorgen voor duidelijkheid. Daarnaast was er onduidelijkheid wie als verantwoordelijke op het gebied van privacybeleid in een organisatie die als 'verantwoordelijke' wordt aangemerkt door de Wbp. Hierdoor ontstond er soms discussie op wie bepaalde rechten of verplichtingen van toepassing zijn. Ook werden veel gegevens in de Wbp als bijzondere gegevens aangemerkt. Meerdere auteurs merkten hierbij op dat of een gegeven een bijzonder gegeven is, afhankelijk is van de context waarin de gegevens worden verkregen en vastgelegd. Tevens werd het feit dat er gedragscodes moesten worden opgesteld voor de verschillende branches en sectoren door auteurs gezien als een knelpunt, omdat dit veel tijd en geld kost. Ook zorgden al deze aparte regelingen samen met de Wbp voor een ontzettend grote regelgeving. Dit heeft als gevolg dat de regelgeving niet eenvoudig te doorgronden is.[15]

Daarnaast was er de kritiek dat een door een organisatie ingestelde Functionaris voor de Gegevensbescherming (FG) misschien niet zo onafhankelijk is, omdat deze door de organisatie zelf ingesteld wordt en omdat het instellen van een FG niet verplicht is. Er werd tevens getwijfeld of het CBP wel genoeg bevoegdheden (tot bijvoorbeeld sancties) heeft als toezichthoudend orgaan. Daarnaast was de CBP gehouden aan een zogenaamde 'doorlooptijd' bij het uitvoeren van onderzoek naar de privacy in bepaalde organisaties. Dit werd door verschillende schrijvers ook als knelpunt ervaren. Sommige auteurs stelden daarnaast dat er in multinationals als knelpunt wordt ervaren dat er verwarring is over bepaalde begrippen, zoals 'persoonsgegevens' bijvoorbeeld.[16]

Ook was er verschil in bedoeling achter het gebruik van bepaalde begrippen tussen de Wbp en andere wetten. Dit was een discussiepunt. Daarnaast hadden de schrijvers de kritiek dat het naleven van de informatieplicht en het naleven van de regels omtrent gegevensbescherming soms botsen. De informatieplicht en het toestemmingsvereiste uit de Wbp zorgden voor ontzettend hoge kosten bij grote organisaties. Ook was er kritiek op het feit dat een belanghebbende zich bij de civiele rechter moet melden om een bepaalde beslissing tegen te gaan. Onder de rechters zou er nog veel kennis ontbreken omtrent de Wbp waardoor de rechters niet eenduidig te werk gaan. Daarnaast was het een grote stap om naar de civiele rechter te stappen, omdat dit erg tijdrovend en duur is. Veel belanghebbenden doen dit daarom niet.[17]

Het tweede onderzoek, genaamd '*Wat niet weet, wat niet deert*', verscheen een jaar later dan onderzoek nummer één. In dit vervolgonderzoek stond de toepassing van de Wbp in de praktijk centraal. Hier werd dus waargenomen of de Wbp de beoogde doelstellingen waarmaakte in de praktijk en op welke wijze knelpunten die uit de theorie naar voren zijn gekomen, zich voordoen in de praktijk. Het onderzoek bestaat uit een enquêteonderzoek en interviews met ervaringsdeskundigen. Omdat de Wbp zo breed opgesteld is, is nadere regelgeving per branche of

[14] WODC 2007, p. 9-10.
[15] WODC 2007, p. 10.
[16] WODC 2007, P. 10-11.
[17] WODC 2007, p. 11-12.

sector van belang. Uit het praktijkgerichte onderzoek bleek dat dit in de helft van de organisaties een dergelijke regeling ontbreekt. Ook was uit het onderzoek gebleken dat de organisaties en betrokkenen het verwerken van persoonsgegevens nog niet als belangrijk aandachtspunt zien. Betrokkenen maakten weinig gebruik van de rechten die zij hebben en stappen nauwelijks naar de rechter. Opvallend was dat slechts bij 0,3% van de organisaties een Functionaris voor de Gegevensbescherming was aangesteld. Het aanstellen van een Functionaris werd door veel organisaties als een te grote stap gezien. De praktijk laat echter wel zien dat er bewuster werd omgegaan met persoonsgegevens. Het meldingsregister van het CBP, waarin de betrokkene een melding kan maken indien deze vindt dat er niet goed met persoonsgegevens wordt omgegaan, was nauwelijks bekend onder de betrokkenen. Hierdoor was het meldingsregister niet als naar behoren werkend aan te merken.[18]

1.1.7 Verloop en huidige stand van de EPV

De datum van inwerkingtreding van de EPV is 25 mei 2016 en de verordening is van toepassing op 25 mei 2018. Er is momenteel dus sprake van een overgangsfase. Organisaties hebben dus nog even de tijd om orde op zaken te stellen en een privacybeleid op te stellen welke compliant is aan de EPV.

1.1.8 Interventiecyclus

De interventiecyclus bestaat uit vijf fases. Een (praktijkgericht) onderzoek kan altijd geplaatst worden in één van deze vijf fases.

1. Probleemsignalering: kan er een probleem ontstaan, welk probleem is dat precies, waarom wordt dit als een probleem ervaren en voor wie is het een probleem?

De eerste fase van de interventiecyclus wordt de probleemsignalering genoemd. Het is namelijk nog niet duidelijk wat het probleem is en het probleem wordt nog niet als zodanig door betrokkenen (vaak de medewerkers en/of het management) erkend. In deze fase dient dus geconcretiseerd te worden of er een probleem kan ontstaan, welk probleem dit is, waarom dit als een probleem wordt ervaren en voor wie dit probleem lastig kan zijn.

2. Diagnose: wat zijn de oorzaken van het probleem, wat zijn de achtergronden, hoe/op welke wijze kan het probleem worden voorkomen, verkleind of opgelost worden?

Bij de diagnose is het probleem als een probleem erkend door de medewerkers en/of het management. Hierna moet de diagnose gesteld worden. Belangrijk is om te kijken naar achtergronden. Hierdoor wordt er inzicht gegeven in de oorzaken van het ontstaan van het probleem.

3. Ontwerp: maken van een plan op basis van de probleemsignalering en de diagnose om tot aanpassingen/verbeteringen te komen (=ontwerp), waarbij rekening moet worden gehouden met vereisten van de omgeving, wet- en regelgeving, toekomstige gebruikers, etc.

De derde fase in de interventiecyclus kan als ontwerpfase aangeduid worden. Er wordt gekeken naar de probleemsignalering en de diagnose. Er moet nu een plan van aanpak gemaakt worden. Hierdoor kan er een oplossing voor het probleem gezocht worden.

4. Interventie: hoe wordt het beoogde veranderingstraject aangepakt, de implementatie conform ontwerp, welke knelpunten zijn er bij de implementatie, is bijsturen (op onderdelen) nodig?

In de derde fase van de interventiecyclus wordt een plan van aanpak gemaakt om tot een oplossing voor het gesignaleerde probleem te komen. In de vierde fase van de interventiecyclus wordt het plan van aanpak gerealiseerd. Hier wordt er dus echt gewerkt aan een oplossing voor het probleem.

5. Evaluatie: is het probleem verkleind of opgelost, is het ontwerp haalbaar en geschikt gebleken, is het ontwerp goed uitgevoerd?

In de laatste fase van de interventiecyclus wordt gekeken of het probleem goed aangepakt is. Er wordt gecontroleerd of de gegeven oplossingen naar behoren werken. Het probleem zou dus

[18] WODC 2008, p. 10-11.

opgelost moeten zijn. Indien dit niet zo is, volgt er bijstelling van het plan van aanpak, waarna er weer een vierde fase en een evaluatie volgt, tot het probleem helemaal opgelost is.[19]

Het onderzoek naar het beleid van het UMCG met betrekking tot het verwerken en beschermen van persoonsgegevens van personeel past in de diagnosticerende fase van de interventiecyclus. Er moet worden geïnventariseerd hoe het bestaande privacybeleid is vormgegeven en wat de knelpunten hierin zijn met oog op de nieuwe EPV. Uiteindelijk zal het huidige beleid waarschijnlijk herschreven en verbeterd moeten worden. Er is, zoals eerder aangegeven, door een jurist van de afdeling juridische zaken van het UMCG een beleidskader opgesteld. In dit beleidskader staan de streefpunten van het UMCG met betrekking tot het privacybeleid en de aandachtspunten van de EPV kort omschreven. Dit beleidskader hoort thuis in de probleemsignalerende fase, omdat hier onderzocht werd wat de EPV inhield en of dit voor problemen kon zorgen voor het UMCG. Het probleem is dus door het UMCG erkend, waardoor dit onderzoek niet in de probleemsignalerende fase zit. Er is echter nog onduidelijkheid over de achtergronden van het probleem. Om dit te bereiken zal het UMCG een privacybeleid moeten gaan hanteren, welke compliant is aan de regelgeving van de EPV. Het beleidskader is weergegeven in bijlage 1 vanaf pagina 72.

1.2 De doelstelling van het onderzoek

Het doen van aanbevelingen aan de Privacy werkorganisatie en de afdeling Juridische Zaken van het UMCG voor het opstellen van een privacybeleid betreffende de afdeling Personeelszaken binnen de kaders van de Europese Privacyverordening
door
het in kaart brengen van het huidige privacybeleid op de afdeling personeelszaken, de eisen die de Europese Privacyverordening aan een privacybeleid stelt en in hoeverre het huidige beleid aanpassingen verdient, door middel van het uitvoeren van een juridisch en niet-juridisch literatuuronderzoek, het onderzoeken van wet- en regelgeving en het houden van interviews met personeelsleden op de afdeling Personeelszaken.

1.3 Centrale onderzoeksvraag

Op welke manier kan het privacybeleid, toegespitst op de afdeling personeelszaken, van het UMCG worden ingericht, zodat deze compliant is aan de bepalingen van de EPV?

1.4. Deelvragen

1. Deelvragen gericht op 'theoretische' bronnen.
- Wat is opgenomen in de huidige wetgeving [Wbp] omtrent het hanteren van privacybeleid?
- Wat is opgenomen in de nieuwe wetgeving [EPV] omtrent hanteren van privacybeleid?
- Wat zijn in theorie belangrijke verschillen tussen de huidige wetgeving en de nieuwe wetgeving omtrent het hebben van privacybeleid?
- Wat is er in de juridische literatuur bekend over de consequenties van de invoering van de EPV voor organisaties?
- Wat is er in de (juridische) literatuur bekend omtrent het opstellen van (privacy)beleid?

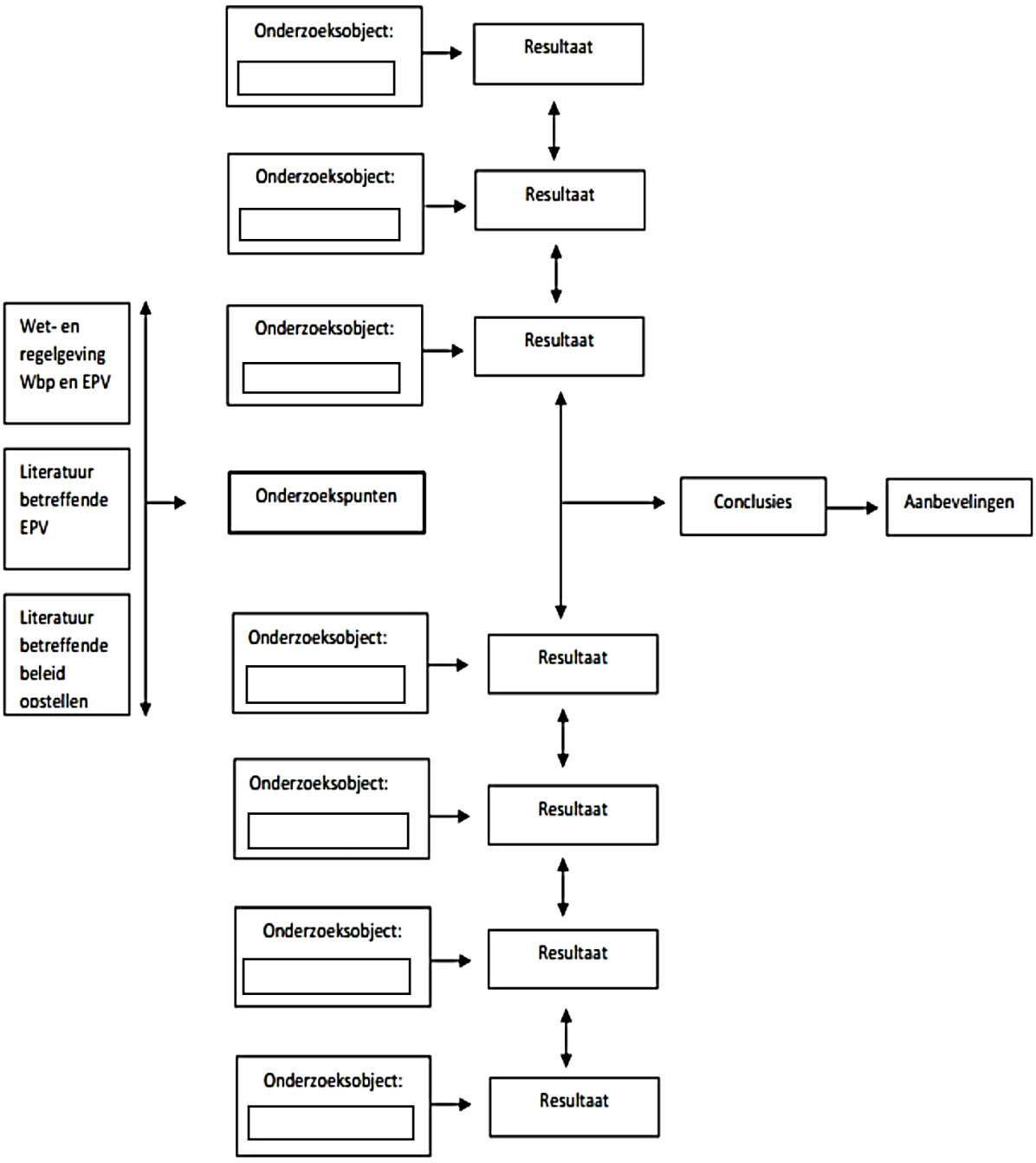
2. Deelvragen gericht op de praktijk (empirie)
- Hoe wordt er op dit moment omgegaan met persoonsgegevens op de afdeling P&O in het UMCG?
- Welk beleid wordt er in de huidige situatie gehanteerd?
- Wat zijn volgens medewerkers van het UMCG aandachtspunten als het gaat om privacy?

3. Deelvragen gericht op analyse
- Wat kan er worden geconcludeerd als de theorie en praktijk met elkaar vergeleken worden?

[19] Verschuren 1995, p. 29 & p. 3.

De deelvragen die gericht zijn op theoretische bronnen zullen worden geanalyseerd en beantwoord worden aan de hand van zowel juridische als niet-juridische literatuurbronnen. Te denken valt aan wetgeving, wetenschappelijke handboeken, beleidsdocumenten van het UMCG en artikelen uit juridische vaktijdschriften. De deelvragen gericht op de praktijk zullen worden beantwoord door middel van verschillende onderzoeksmethoden. Er wordt hier veel gebruik gemaakt van het afnemen van interviews. Dit zorgt namelijk voor opheldering over het beleid dat er op dit moment is en hoe hiermee omgegaan wordt. Daarnaast zijn er nog deelvragen die gericht zijn op het analyseren van de hierboven aangehaalde twee soorten deelvragen. In het antwoord op deze deelvragen vindt er een vergelijking plaats tussen de theorie en praktijk. Op basis van de theorie worden namelijk onderzoekspunten geformuleerd welke vervolgens in de praktijk worden getoetst. Deze toetsing zal uiteindelijk leiden tot de onderzoeksresultaten, namelijk de conclusies en aanbevelingen die gegeven zullen worden aan de hand van dit onderzoek.

1.5 Onderzoeksmodel



2. Methodologische verantwoording

In de methodologische verantwoording wordt ingegaan op de onderzoeksmethoden en de validiteit van het onderzoek.

2.1 Onderzoeksmethoden

In dit onderzoek is er gebruik gemaakt van verschillende onderzoeksmethoden. Deze onderzoeksmethoden hebben geholpen met het beantwoorden van de deelvragen. Met het beantwoorden van de deelvragen is uiteindelijk antwoord gegeven op de hoofdvraag. In dit hoofdstuk wordt informatie gegeven over de gebruikte onderzoeksmethoden en de wijze waarop deze hebben geholpen met het onderzoeken.

Voor het theoretische gedeelte van het onderzoek is gebruik gemaakt van wet- en regelgeving, kamerstukken en (niet-)juridische literatuur. Deze zijn in het vooronderzoek bij elkaar gezocht en bestudeerd. In het theoretische deel van het onderzoek is deze literatuur geanalyseerd door middel van een juridische inhoudsanalyse. Dit is een onderzoeksmethodologie waarbij relevante rechtsbronnen en juridische literatuur bestudeerd worden, zodat er na afronding van de analyse valide conclusies getrokken kunnen worden. Op basis van de theorie konden onderzoekspunten worden geformuleerd. Er is gebruik gemaakt van niet-juridische literatuur betreffende het privacybeleid binnen organisaties. Er is geen gebruik gemaakt van jurisprudentie aangezien de EPV nog niet in werking is getreden. Er is daarom nog geen relevante jurisprudentie aanwezig. De jurisprudentie met betrekking tot de Wbp was niet van toegevoegde waarde voor het onderzoek.

Voor het praktijkgedeelte is gedeeltelijk deskresearch gedaan. Het privacyreglement dat geldend is op de afdeling P&O, is vergeleken met de bepalingen van de EPV. Er wordt in de EPV misschien weinig ingegaan op het verplichte privacybeleid, maar op grond van de EPV moeten de bepalingen in het privacybeleid compliant aan de EPV zijn en zo uitgevoerd worden. Alle bepalingen van de EPV moeten dus in acht worden genomen. Tevens is het kaderbeleid 'Privacybeleid UMCG' bestudeerd, waarin de doelen en de uitgangspunten van het UMCG nader toegelicht worden. Deze is opgesteld door een jurist, werkzaam op de afdeling Juridische Zaken van het UMCG. Deze is juridisch opgeleid en kent het UMCG als organisatie. Om deze redenen kan de betrouwbaarheid van dit stuk aangenomen worden.

Daarnaast is er voor het praktijkgedeelte gebruik gemaakt van kwalitatief onderzoek in de vorm van interviewgesprekken. Door middel van kwalitatief onderzoek kan er diep ingegaan worden op achterliggende motivaties, wensen, meningen en behoeften van de doelgroep. Zowel bewuste als onbewuste gedachten en gedragingen op de afdeling P&O kunnen hierdoor in kaart worden gebracht. Het uitvoeren van een kwalitatief onderzoek heeft enkele voordelen: de onderzoeker heeft de kans om door te vragen en de vragen kunnen aangepast worden indien de resultaten van het interview hierom vragen. Hierdoor kan er door de onderzoeker ingespeeld worden op bepaalde resultaten, waardoor eventuele remmingen weggenomen kunnen worden bij respondenten. Deze konden hierdoor vrijuit hun mening geven. Tevens kon door de keuze van kwalitatief onderzoek doorgevraagd worden naar eventuele implementatie van een nieuw privacybeleid. Het overstaande van kwalitatief onderzoek is kwantitatief onderzoek. Dit is bijvoorbeeld een enquête. Er kan tijdens een enquête minder diep ingegaan worden op het onderwerp. Het voordeel van een goede enquête is dan wel weer dat deze statistisch representatief zijn.[20] Hier is niet voor gekozen omdat de onderzoeker diep op ervaringen, gedachten en meningen van de respondenten in wilde gaan en remmingen wilde wegnemen bij respondenten. Dit kan beter bereikt worden door middel van interviews dan door middel van een enquête.

[20] Right marktonderzoek 2016.

Van belang was niet alleen om te achterhalen of er een schriftelijke privacybeleid was, maar ook of deze goed werkend was op de afdeling P&O. Meningen en behoeften van medewerkers en leidinggevenden met oog op een nieuw privacybeleid en de nieuwe wetgeving spelen mee. Om dit zo zorgvuldig mogelijk in kaart te kunnen brengen zijn er respondenten geïnterviewd met verschillende functies. Wel hadden al deze functies betrekking tot de afdeling P&O. De afdeling P&O is opgedeeld in verschillende sectoren, waar telkens persoonsgevens worden verwerkt per functie van de medewerker. De geselecteerde respondenten die hebben meegewerkt aan een interview worden hieronder weergegeven:

Naam
Respondent 1
Respondent 2
Respondent 3
Respondent 4
Respondent 5
Respondent 6
Respondent 7

Tabel 1 Respondenten

De respondenten hebben allemaal banden met de afdeling P&O. De keuze voor medewerkers van deze afdeling was logisch, omdat het hele onderzoek is toegespitst op deze personeelsafdeling. Er is gekozen voor verschillende sectoren, om een zo breed mogelijk kader aan informatie te verkrijgen. Daarnaast is er gekozen voor verschillende functies, omdat een eventueel komend privacybeleid op verschillende niveaus op de afdeling P&O geïmplementeerd moet worden en goed werkend moet zijn.

In totaal zijn er zeven interviews, elk met één respondent, afgenomen. Elk interview bestond uit vooraf opgestelde vragen, waarbij eerst gevraagd werd welke functie de respondent bekleedde en hoelang deze al in de functie werkzaam is. Er is gekozen om dezelfde soort vragen te stellen, zodat de gegeven resultaten met elkaar vergeleken konden worden. Deze vragen zijn opgesteld op basis van de onderzoekspunten. Indien er telkens andere vragen gesteld zouden worden, is een goede vergelijking bijna onmogelijk. Naast deze openingsvragen is er ingegaan op het hanteren van privacybeleid op de afdeling P&O. In kaart gebracht moest worden of er sprake is van een schriftelijk privacybeleid en/of er sprake is van ongeschreven beleid met betrekking tot het verwerken van persoonsgegevens. Vooraf is besloten dat indien er sprake zou zijn van een schriftelijk beleid, direct gevraagd moest worden of deze aan de onderzoeker verstrekt kon worden. Tevens zijn er vragen gesteld over de bepalingen van de EPV, en dan vooral de rechten van de betrokkenen en de verplichtingen die het UMCG als organisatie heeft. In kaart moest worden gebracht of de EPV als onderwerp leeft binnen de afdeling en hoeveel de respondenten over de EPV konden vertellen. Er is gekozen om zoveel mogelijk open vragen te stellen, zodat er zoveel mogelijk informatie naar boven zou komen en de respondenten in staat gesteld werden om hun gedachtengoed te delen.

De interviewer heeft gekozen voor een half gestructureerd interview. Hierdoor kon de interviewer doorvragen. Dit komt ten goede aan de diepgang van het gesprek. Ondanks dat de vooraf opgestelde vragen de leidraad waren in het gesprek, was er voor de respondent elke keer veel vrije ruimte om ervaringen, gedachten en kennis over privacybeleid op de afdeling P&O te delen. Om te zorgen dat de interviewer alle aandacht kon besteden aan het voeren van het gesprek zijn de gesprekken opgenomen met een dictafoon.
Hierdoor was er geen afleiding door het gelijk moeten noteren van antwoorden. Voor de start van het interview is toestemming gevraagd aan de respondenten voor de opname. De spraakopnames zijn thuis afgeluisterd na afloop van de gesprekken. De antwoorden zijn met elkaar vergeleken en de relevante antwoorden zijn verwerkt in de praktijkresultaten waarmee de onderzoekspunten zijn getoetst.

2.2 Validiteit

Theorie

Voor het opstellen van het theorie gedeelte is alleen gebruik gemaakt van hoogstaande literatuur. Dit bestond uit vaktijdschriften en boeken geschreven door auteurs met een juridische achtergrond. Het theoriegedeelte is gebaseerd op de laatste en vastgestelde versie van de EPV. De EPV wettekst zal niet meer aangepast worden, waardoor de gebruikte wettekst gegarandeerd valide is. Daarnaast zijn de beleidsregels van de Autoriteit Persoonsgegevens gebruikt in het theoriegedeelte. Deze beleidsregels zijn opgesteld door de Autoriteit Persoonsgegevens en geven kijk op de werkwijze van deze nationale toezichthouder. Omdat deze beleidsregels van de organisatie zelf komen zijn deze erg betrouwbaar. Verder is er gebruik gemaakt van enkele websites. Allereerst is er een website gebruikt van een advocatenkantoor. Het artikel dat gebruikt is, is geschreven door een advocaat welke specialist is op het gebied van Europese wetgeving. Daarnaast is er gebruik gemaakt van de website van Right marktonderzoek. Right marktonderzoek is een professioneel marktonderzoeksbureau, welke ook opdrachten heeft uitgevoerd voor Universiteiten, Provincies en het Ministerie. Van deze organisatie is aan te nemen dat deze kennis heeft op het gebied van onderzoeksmethoden. De laatste website die is gebruik is de website van de Nederlandse Vereniging Ziekenhuizen. De Nederlandse Vereniging Ziekenhuizen behartigt de collectieve zorginhoudelijke, sociale en economische belangen van ziekenhuizen. Aangenomen kan worden dat deze nationale vereniging valide is met betrekking tot informatie op het gebied van zorginstellingen. Mijns inziens is het theoriegedeelte zeer valide van aard.

Praktijk

Er moet gekeken worden naar verschillende aspecten om te beoordelen of de kwalitatieve methode van onderzoek adequaat genoeg is om conclusies uit te kunnen trekken. De respondenten hadden verschillende soorten functies met betrekking tot de afdeling P&O. Met de P&O adviseurs van drie verschillende sectoren, A, C en D, is gesproken. Deze sectoren hadden te maken met het verwerken van gegevens van medewerkers, waar dit onderzoek op toegespitst is. Er was verschil in het werkniveau en opleiding van de respondenten. Zo kon er in kaart gebracht worden of de komst van de EPV zowel boven in de organisatie (de hoofden en leidinggevenden) als onder in de organisatie (medewerkers) leefde. Er is daarnaast veel contact geweest met de Privacy werkorganisatie, welke inhoudelijk het werk op het gebied van privacy uitvoert binnen het UMCG. Zij hebben besloten welke respondenten geïnterviewd zouden worden, omdat zij wisten welke medewerkers van belang waren voor dit onderzoek.

Om vast te kunnen stellen hoe betrouwbaar de interviews zijn, moet gekeken worden of het kwalitatieve onderzoek intersubjectief is. Het is met oog daarop van belang om vast te stellen of de interviewer de resultaten op eniger wijze heeft beïnvloed, doordat deze niet objectief is geweest tijdens de interviews. Een objectieve interviewer laat zich niet leiden door resultaten uit eerdere interviews, vooroordelen en ervaringen. De onderzoeker heeft objectiviteit getracht te bereiken door vooraf opgestelde interviewvragen te gebruiken en de respondent zoveel mogelijk te laten vertellen. Hierdoor kon de interviewer het gesprek minder sturen op grond van antwoorden uit eerdere interviews, maar moest deze zich vasthouden aan de vooraf opgestelde vragenlijst. Deze vragenlijst is niet veranderd gedurende het praktijkonderzoek om objectiviteit na te streven.

Er kan echter wel enigszins gestuurd zijn door de interviewer tijdens de laatste interviews, omdat de interviewer ervoor gekozen heeft door te vragen. De wijze van doorvragen kan beperkt beïnvloed zijn door ervaring en kennis die is opgedaan door eerder gehouden interviews. Er is nauwelijks tot geen informatie verloren gegaan omdat de interviews getranscribeerd zijn. De resultaten uit het onderzoek kunnen zeer betrouwbaar genoemd worden. Er is met een talrijk aantal respondenten gesproken, die allen functies vertegenwoordigen die betrekking hebben op de afdeling P&O. Het enige punt dat afdoet aan de betrouwbaarheid is dat de interviewer na het vijfde interview op de

hoogte was van het bestaan van het privacyreglement en haar bepalingen. Hierdoor heeft de interviewer mogelijk aangestuurd bij de twee volgende gesprekken dat er een privacyreglement is, om te achterhalen hoe het kan dat de medewerker hier misschien niets vanaf weet of niet weet welk stuk er bedoeld wordt. Hierdoor kreeg het gesprek een gevolg, om zodoende meer informatie uit de medewerkers te krijgen. De interviewer heeft ervoor gekozen het privacyreglement niet te bekijken tot afloop van de interviews, zodat onbewuste sturing van het gesprek in de richting van bepaalde bepalingen van het reglement voorkomen kon worden.

2.3 Terugblik

Als ik terug kijk naar het onderzoek ben ik tevreden over de onderzoeksmethoden die ik in samenspraak met mijn praktijkbegeleider heb gekozen. Het theoriegedeelte is mijn inziens erg valide omdat ik gebruik heb gemaakt van betrouwbare literatuur. Alle auteurs zijn vakmensen op hun eigen gebied. Door het gebruik van deze literatuur heb ik tijdens mijn onderzoek geleerd dat het gebruikmaken betrouwbare literatuur een ware toevoeging is voor het doen van onderzoek en mijn eigen kennis. Ik ben erg tevreden over de gesprekken die ik met alle respondenten heb gevoerd. Er was elke keer weer sprake van een ‘natuurlijke’ gesprekssituatie. Hierdoor zijn er veel meer informatie, ervaringen en meningen naar boven gekomen dan wanneer ik gebruik had gemaakt van een enquête of een geforceerde gesprekssfeer. Ik heb er van te voren goed over na gedacht hoe ik dit wilde gaan aanpakken en mijns inziens heb ik hier de juiste keuzes in gemaakt.

3. Wet Bescherming Persoonsgegevens

In de volgende hoofdstukken zal er uiteenzetting van theorie plaatsvinden.
De theorie die hieronder beschreven wordt is gericht op de deelvraag:
- *Wat is opgenomen in de huidige wetgeving (Wbp) omtrent het hanteren van privacybeleid?*

3.1 Belangrijke begrippen

In artikel 1 van de Wbp worden de begrippen uitgelegd die voor deze wet belangrijk zijn. Deze wettelijke definitie is soms ietwat aan de korte kant. Er zal daar een nadere toelichting plaatsvinden.

3.1.1 Persoonsgegevens

In de Wbp wordt het begrip persoonsgegevens aangeduid als '*elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon*'. Opvallend aan deze definitie is dat er de term 'natuurlijk persoon' wordt gehanteerd. De wetgever wil hiermee duidelijk maken dat onder persoonsgegevens in de Wbp nooit de gegevens van een rechtspersoon verstaan kunnen worden. Daarnaast is het opvallend dat deze gegevens identificeerbaar dienen te zijn. Hiermee wordt bedoeld dat de gegevens terug gevoerd kunnen worden op een persoon. Het begrip 'persoonsgegevens' is een ruim begrip, waar vele soorten gegevens onder vallen. Voorbeelden van een persoonsgegeven zijn iemands leeftijd, woonplaats, adres, postcode en telefoonnummer.[21]

Het persoonsgegeven moet identificeerbaar zijn aan een natuurlijk persoon. Het vereiste dat er sprake van een natuurlijk persoon moet zijn, gaat niet altijd op. Ook gegevens over bijvoorbeeld gebeurtenissen en goederen kunnen als persoonsgegevens worden beschouwd. Voorwaarde hiervoor is dat deze gegevens informatie bevatten die betrekking heeft op natuurlijke personen. Over andere gegevens kan onduidelijkheid bestaan. Geldend is hier dat indien er een reële kans is dat gegevens (ook) betrekking hebben op een natuurlijk persoon, deze gegevens ook als persoonsgegevens aangeduid kunnen worden. Zo is een kenteken van een auto een persoonsgegevens, omdat deze informatie bevat over de eigenaar van de auto en dat is een natuurlijk persoon. Voor al het bovenstaande geldt wel dat de gegevens identificeerbaar moeten zijn. De identiteit van de eigenaar van de auto uit het voorbeeld, zal herleidbaar moeten zijn om dit als een persoonsgegeven aan te kunnen merken. Alleen gegevens die zodanig zijn geanonimiseerd dat ze helemaal niet meer te herleiden zijn naar een persoon, zijn geen persoonsgegevens.[22]

Er wordt in de Wbp onderscheid gemaakt tussen direct identificeerbare en indirecte identificeerbare persoonsgegevens. Een direct identificeerbaar persoonsgegeven is een persoonsgegeven waarmee de identiteit van een persoon heel eenvoudig te achterhalen is. Voorbeelden hiervan zijn de naam en de geboortedatum van een persoon. Bij indirect identificeerbare persoonsgegevens ligt dit anders. Deze gegevens leiden niet direct tot identificatie van iemand, maar met nadere stappen kan wel achterhaald worden aan wie de gegevens toebehoren, zoals het aangehaalde voorbeeld van het kenteken van de auto. Er zijn ook nog gegevens die erg uniek per persoon zijn, en daarmee identificerend, zoals een DNA-profiel.[23]

3.1.2 Verwerking van persoonsgegevens

In de Wbp wordt de verwerking van persoonsgegevens omschreven als '*elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van*

[21] Berkvens 2007, p. 104.
[22] Berkvens 2007, p. 81-82.
[23] MvT Wbp, p. 48.

gegevens'. Zodra er sprake is van een persoonsgegeven en hier wordt iets mee gedaan, zal er al snel gesproken kunnen worden van verwerking. Dit komt omdat er sprake is van een heel ruim begrip.[24]

3.1.3 Bijzondere gegevens

Bij bijzondere gegevens moet gedacht worden aan gegevens die gevoelig kunnen liggen bij de betrokkene. Voorbeelden hiervan zijn gegevens omtrent de godsdienst, levensovertuiging, ras, politieke voorkeur, seksuele leven en de medische toestand van een persoon. Omdat deze gegevens zo gevoelig kunnen liggen, zijn er zwaardere eisen in de Wbp opgenomen voordat organisaties deze gegevens mogen verwerken.[25] De bijzondere gegevens zijn naar soort opgedeeld in categorieën. Per categorie zijn er extra nadere regels opgenomen in de Wbp.[26]

3.1.4. De betrokkene

In de Wbp wordt er van de 'betrokkene' gesproken indien het gaat om *'degene op wie een persoonsgegeven betrekking heeft'*. Een voorbeeld is een patiënt van het UMCG waarvan gegevens worden opgeslagen. De betrokkene heeft in de Wbp bepaalde rechten gekregen. Een voorbeeld van deze rechten is het recht van de betrokkene om persoonsgegevens in te zien die op hem of haar van toepassing zijn en opgeslagen zijn bij een organisatie.[27]

3.1.5 De verantwoordelijke

In de Wbp wordt het begrip 'verantwoordelijke' omschreven als '*de natuurlijke persoon, rechtspersoon of ieder ander die of van het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt'*. Het doel van de wetgever met deze ruime wetsbepaling is duidelijk dat het toepassingsgebied zo groot mogelijk wordt gemaakt. Hierdoor zal er snel gesproken kunnen worden van een verantwoordelijke en heeft deze zich aan de wetsbepalingen van de Wbp te houden. Omdat iemand zo snel aangemerkt kan worden als verantwoordelijke voor de Wbp, is het belangrijk om goed te regelen wie de verantwoordelijke en wie de bewerker is. Dit in verband met aansprakelijkheid. Meer over het begrip 'bewerker' kan hieronder gelezen worden.[28]

Wie als verantwoordelijke aangewezen wordt, is afhankelijk van het doel van de verwerking. Dit doel wordt namelijk door de verantwoordelijke vastgesteld. Daarnaast bepaalt de verantwoordelijke met welke middelen dit doel de persoonsgegevens worden verwerkt. De Wbp richt zich hier op wie formeel juridisch verantwoordelijk is voor deze verwerking. De verantwoordelijke kan zowel een natuurlijk persoon als rechtspersoon zijn. Als het gaat om de overheid is de verantwoordelijke het bestuursorgaan. Indien er geen sprake is van overheid is de verantwoordelijke vaak een rechtspersoon. Echter, indien er sprake is van een eenmanszaak kan een natuurlijk persoon ook als verantwoordelijke aangemerkt worden. De verantwoordelijkheid kan tevens gedragen worden door twee bestuursorganen of rechtspersonen. Dit is bijvoorbeeld het geval indien meerdere verantwoordelijke belang hebben bij het verwerken van een persoonsgegeven.[29]

Er kan volgens de toelichting van de Wbp sprake zijn van 3 soorten verantwoordelijkheid:

- Er kan sprake zijn van gezamenlijke verantwoordelijkheid waarbij er meerdere verantwoordelijken zijn, die elk ongeveer evenveel verantwoordelijkheid dragen voor het geheel.

[24] Artikel 1 sub b Wbp.
[25] Artikel 16 Wbp.
[26] Artikel 17-22 Wbp.
[27] Artikel 1 sub f Wbp.
[28] Berkvens 2007, p. 105.
[29] Berkvens 2007, p. 85.

- Daarnaast kan er sprake zijn van gedifferentieerde verantwoordelijkheid. Ook hier is er sprake van meerdere verantwoordelijken, alleen nu heeft ieder een stuk verantwoordelijkheid voor een aantal verwerkingen. Deze stukken verantwoordelijkheid kunnen op verschillende manieren verdeeld zijn, zoals bijvoorbeeld op geografie, op soort of op type. Hierbij is niet elke verantwoordelijke verantwoordelijk voor het geheel, zoals bij gezamenlijke verantwoordelijkheid, maar alleen voor het stuk dat aan haar toebedeeld is.
- Tevens kan er één gemeenschappelijke verantwoordelijke zijn, ondanks de aanwezigheid van meerdere organisaties die deelnemen of opdracht geven voor de verwerkingen. Vaak zijn er hier een aantal partijen die de verwerking van persoonsgegevens hebben uitbesteed aan een derde. De gemeenschappelijke verantwoordelijke is aansprakelijk voor het geheel. De andere organisaties moeten er wel voor zorgen dat zij de (persoons)gegevens goed aanleveren.[30]

3.1.6. De bewerker

In de Wbp wordt de 'bewerker' omschreven als *'degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen'*. Hieruit is af te leiden dat de bewerker gegevens verwerkt voor de verantwoordelijke. Dit kan bijvoorbeeld op basis van een overeenkomst te zijn. Toch blijft het in sommige gevallen vaag wat precies onder dit begrip valt. Er gelden in de hele Europese Unie ongeveer dezelfde regels. Indien de bewerker buiten de Europese Unie is gevestigd gelden deze regels niet automatisch. Het is dan de taak van de verantwoordelijke om ook daar te zorgen voor een goede beveiliging van de persoonsgegevens. Zoals bij de 'verantwoordelijke' besproken, is het belangrijk om de aansprakelijkheid goed te regelen. Aanbevolen kan worden om dit door een gespecialiseerde jurist te laten doen in de vorm van een schriftelijke overeenkomst, omdat dit erg ingewikkeld kan zijn.[31] Voor afbakening van de relatie van de verantwoordelijke en de bewerker is de zeggenschap en het bepalen van de doelstellingen beslissend. De bewerker verwerkt de persoonsgegevens zonder zeggenschap te hebben over het doel van de verwerking. Indien de bewerker deze zeggenschap wel heeft kan hij derhalve aangemerkt worden als verantwoordelijke. De details van de verwerkingswijze kunnen wel aan de bewerker overgelaten worden, zonder dat deze gelijk als verantwoordelijke aangemerkt wordt.[32]

3.1.7 Toestemming van de betrokkene

Toestemming van de betrokkene wordt in de Wbp omschreven als *'elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt'.*

3.2 Beginselen

Allereerst is het transparantiebeginsel een belangrijk beginsel van de Wbp. De betrokkene heeft het recht om controle te hebben over zijn eigen gegevens. Dit kan alleen als organisaties transparant en open te werk gaan. Hieronder valt dat de organisatie de persoonsgegevens alleen opslaat, deelt en verwerkt indien de betrokkene daarvan op de hoogte is. Tevens dient de betrokkene te weten voor hoelang dit is. [33]

De verantwoordelijke organisatie dient ook aan de betrokkene mee te delen voor welk doel de gegevens worden verwerkt. Dit valt onder het doelbindingsbeginsel. De verantwoordelijke organisatie moet vooraf bepalen en uitdrukkelijk omschrijven welke gegevens verwerkt worden. Daarnaast dient het doel de verwerking van de gegevens te rechtvaardigen. Het verwerken van persoonsgegevens is alleen gerechtvaardigd indien de verwerking voldoet aan de doeleinden die in de Wbp staan. De doeleinden op grond waarvan de verantwoordelijke de gegevens kan verwerken

[30] Berkvens 2007, p. 86.
[31] Berkvens 2007, p. 105.
[32] Hustinx 2002, p. 1-2.
[33] Duthler 2013, p. 9.

zijn: indien de betrokkene ondubbelzinnig toestemming heeft verleend voor de verwerking van zijn of haar persoonsgegevens, indien de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst met de betrokkene, indien de verwerking noodzakelijk is voor de verantwoordelijke om wettelijke verplichtingen na te komen, indien de gegevensverwerking noodzakelijk is voor de vervulling van een publiekrechtelijke taak door een bestuursorgaan, en indien de gegevensverwerking noodzakelijk is voor een gerechtvaardigd belang, tenzij het belang, de rechten of de vrijheden van de betrokkene prevaleren. [34] Een derde beginsel is het evenredigheidsbeginsel. Dit beginsel ziet erop toe dat de inbreuk op de belangen van de betrokkene niet onevenredig is aan het doel waarvoor de gegevens verwerkt worden. Het laatste belangrijke beginsel waar de Wbp op voortborduurt is het subsidiariteitsbeginsel. Op grond van dit beginsel mogen gegevens alleen verwerkt worden indien het doel waarvoor deze verwerkt worden niet op een andere manier kan worden bereikt.[35]

3.3 Reikwijdte

De reikwijdte van de Wbp is beschreven in de beginartikelen van de Wbp zelf. Hieruit volgt dat de Wbp van toepassing is op de verwerking van persoonsgegevens door een verantwoordelijke die in Nederland is gevestigd. De Wbp geldt voor een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens. De Wbp is ook van toepassing op de niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of worden opgenomen. De Wbp is niet van toepassing op artikelen die persoonsgegevens verwerken voor journalistieke, artistieke of literaire doeleinden. Indien de verantwoordelijke geen vestiging in de Europese Unie heeft, kan de Wbp alsnog van toepassing zijn, namelijk als er met de verwerking van de persoonsgegevens gebruik wordt gemaakt van middelen die zich in Nederland bevinden. Dit is niet het geval indien de middelen die zich in Nederland bevinden alleen gebruikt worden als doorvoer.[36]

Het onderwerp van de Wbp is het verwerken van persoonsgegevens.[37] Zoals hierboven omschreven bij de belangrijke begrippen, dient er voor toepassing van de Wbp sprake te zijn van een persoonsgegeven en van verwerken hiervan. In paragraaf 3.1.1 is besproken wanneer er sprake is van een persoonsgegeven. Verwerking is een ruim begrip. Er zijn ontzettend veel handelingen die als verwerking kunnen worden gezien. In de lijst met belangrijke begrippen worden de meest voor de hand liggende vormen van verwerking vermeld. Er kan sprake zijn van primaire of secundaire handelingen die onder verwerking vallen. De primaire handelingen worden omschreven als *'het gebruik van persoonsgegevens voor het beoogde doel'* en de secundaire handelingen worden omschreven als *'handelingen die bijdragen aan de primaire handeling'*. Het verschil tussen primaire en secundaire handelingen is niet van belang voor het bepalen of er sprake is van verwerking. Beide soorten handelingen vallen onder het begrip. [38]

3.4 Verwerking van medische informatie

Om meer te weten te komen over privacy en medische informatie is het eerst van belang om te weten wat medische informatie precies is. Medische informatie wordt beschreven als *'alle gegevens betreffende iemands lichamelijke of geestelijke gezondheid in het verleden, heden of in de toekomst, inclusief genetische gegevens'.* Omdat het hier vaak over gevoelige informatie gaat, zijn er bepalingen opgenomen in de Wbp die nadere regels stellen aan de verwerking van medische gegevens. Het medisch beroepsgeheim is al een belangrijk instrument als het gaat om privacyregulering. Hulpverleners mogen op grond van hun beroepsgeheim geen informatie over een

[34] Artikel 7-8 Wbp.
[35] Mvt Wbp, p.80.
[36] Artikel 2-4 Wbp.
[37] Berkvens 2007, p. 81.
[38] Berkvens 2007, p. 83.

patiënt, aan ieder ander dan aan de patiënt zelf, verstrekken. Het verstrekken van informatie aan een andere hulpverlener mag wel indien dit noodzakelijk is voor het uitvoeren van de behandeling. Het beroepsgeheim geldt voor alle informatie die de hulpverlener door zijn of haar werk te weten komt. Alleen op grond van een wettelijke verplichting of met toestemming van de patiënt mag de hulpverlener van afstand doen van zijn zogenaamde zwijgplicht.[39] Medische gegevens vallen onder de zogenaamde 'bijzondere persoonsgegevens'. In de Wbp wordt verboden om medische gegevens of gegevens over iemands gezondheid te verwerken. Gegevens over iemands ras of geloofsovertuiging kunnen hier soms onder vallen, indien deze verband houden met zijn of haar medische toestand. Er zijn echter wel uitzonderingen op de regel dat medische gegevens niet verwerkt mogen worden. Bepaalde instanties mogen dat namelijk wel doen. Het gaat hier om hulpverleningsinstanties, instellingen of voorzieningen voor de gezondheidszorg of maatschappelijke dienstverlening. De verwerking mag echter alleen plaatsvinden indien dit noodzakelijk is voor de behandeling van de betrokkene. Andere soort instanties die medische gegevens mogen verwerken staan in het Wbp zelf, maar zijn niet van belang voor de afdeling P&O. Medische gegevens mogen alleen verwerkt worden door personen met een geheimhoudingsplicht. Er zijn uitzonderingen op de verwerkingsverboden, namelijk als de betrokkene uitdrukkelijk instemt met de verwerking.[40]

Niet alleen het Wbp ziet toe op de verwerking van medische gegevens. Ook het Burgerlijk Wetboek (BW) bevat enkele bepalingen omtrent privacy en medische informatie. Waar het Wbp gericht is op privacy, is het overeenkomstenrecht van het BW dit niet specifiek. De privacy van de patiënt is hier meer een deel van een grotere overeenkomst. De regeling in het BW is meer gericht op de verhouding tussen patiënten en hulpverleners. Het gaat hier om de privaatrechtelijke verhouding.[41] Dit wordt de Wet op de Geneeskundige Behandelingsovereenkomst genoemd (Wgbo). Deze wet regelt dat het dossier dat de hulpverlener houdt binnen drie maanden na een verzoek van de patiënt verwijderd dient te worden. Daarnaast bepaalt de Wgbo dat de patiënt op verzoek zo snel mogelijk inzage dient te krijgen in zijn of haar dossier. Anderen dan de patiënt zelf kunnen alleen inlichtingen krijgen omtrent (de zorg van) de patiënt en inzage krijgen in het dossier van de patiënt, als de patiënt hiervoor toestemming heeft gegeven. Onder anderen dan de patiënt vallen niet personen die rechtstreeks betrokken zijn bij de uitvoering van de overeenkomst of de vervanger van de hulpverlener. Deze verkrijgen echter niet meer informatie dan noodzakelijk is. De bepalingen in het BW op het gebied van privacy doen niet onder voor de bepalingen in de Wbp. Deze werken namelijk naast elkaar.[42]

3.5 Privacybeleid

In de Wbp is het hanteren van een privacybeleid in de verantwoordelijke organisatie niet verplicht gesteld. Organisaties kunnen dus zelf de keuze maken of zij een intern privacybeleid opstellen en toepassen.

3.6 Gegevensverwerking medewerkers

In de Wbp zijn regels opgenomen omtrent het verwerken van persoonsgegevens van medewerkers. Het onderzoek is toegespitst op de afdeling P&O. Deze personeelsafdeling verwerkt persoonsgegevens van werknemers. De Wbp geeft de voorwaarden voor het aanleggen van personeelsdossiers.[43]

Voor het verwerken van persoonsgegevens moet een verantwoordelijke organisatie een rechtsgrondslag hebben. Toestemming van de betrokkene kan zo'n rechtsgrondslag zijn.

[39] Berkvens 2007, p. 255-257.
[40] Artikel 16-23 Wbp.
[41] Berkvens 2007, p. 262.
[42] Artikel 7:453- 7:457 BW.
[43] Artikel 22 lid 3 Wbp.

In de Memorie van Toelichting (MvT) van de Wbp werd omschreven wanneer er sprake is van toestemming. Allereerst moet de betrokkene in vrijheid zijn wil over de gegevensverwerking kunnen uiten. Daarnaast moet deze wilsuiting betrekking hebben op een bepaalde gegevensverwerking of een beperkte categorie hiervan. Het moet daarom duidelijk zijn over welke verwerking het gaat, welke gegevens verwerkt zullen worden en met welk doel de gegevens verwerkt worden. Tevens dient de betrokkene waarvan toestemming voor gegevensverwerking wordt verkregen, goed ingelicht te zijn. Als de betrokkene niet goed ingelicht is, biedt de toestemming geen grondslag voor gegevensverwerking. Volgens de MvT van de Wbp kan er niet van rechtsgeldige toestemming worden gesproken indien de betrokkene onder druk van de relatie waarin hij staat tot de verantwoordelijke tot toestemming is overgegaan. Een voorbeeld van een relatie die deze druk tot toestemming bij de betrokkene kan veroorzaken, is de arbeidsrelatie. Er is sprake van een gezagsverhouding en de werkgever betaald de werknemer loon als tegenprestatie voor zijn werkzaamheden. Aanzienlijke onevenwichtigheid is dan eenvoudig aan te nemen.[44]

Uit bovenstaande informatie kan geconcludeerd worden dat de afdeling P&O toestemming van de betrokkene, de werknemer, niet als voorwaarde voor de verwerking van persoonsgegevens mag gebruiken. De afdeling P&O kan de persoonsgegevens van de medewerkers verwerken op grond van de arbeidsovereenkomst die zij met de medewerkers heeft. Voor de arbeidsovereenkomst is het namelijk noodzakelijk op bepaalde gegevens van de medewerker te verwerken. De Wbp geeft deze mogelijkheid.[45]

3.7 Handhaving

De handhaving wordt volgens de Wbp uitgevoerd door twee organen, het College Bescherming Persoonsgegevens (CBP) en de Functionaris voor de Gegevensbescherming (FG). Het CBP is een extern toezichtorgaan en de FG is een intern toezichtorgaan. Het CBP is in 2001 ingesteld om te bevorderen dat de privacy van betrokkenen volgens de bepalingen van het Wbp worden nageleefd. Het CBP heet sinds 1 januari 2016 Autoriteit Persoonsgegevens (AP).

In de Wbp zijn regels opgenomen omtrent het werkproces van de AP. De AP heeft vier wegen uitgestippeld om haar doel als toezichts- en handhavingsorgaan te bereiken. Achtereenvolgens zijn deze vier wegen; bewustwording, normontwikkeling, technologie en handhaving. Met bewustwording wordt privacybewustzijn bedoelt. De bedoeling is om met voorlichting en communicatie te zorgen dat betrokkenen en verantwoordelijke organisaties bewust bezig gaan met privacy. Betrokkenen moeten weten wat hun rechten zijn en verantwoordelijke organisaties moeten weten wat hun plichten zijn. De AP doet dit door voorlichting te geven op hun internetwebsite en door vragen te beantwoorden die partijen hebben. Met normontwikkeling wordt bedoeld dat de AP de bestaande normen omtrent de verwerking van persoonsgegevens verder gaat concretiseren en ontwikkelen. Daaropvolgend doet de AP aanbevelingen aan de regering over de werking van de Wbp.[46]

De AP adviseert daarnaast bepaalde organisaties omtrent de door hun opgestelde gedragscodes. Dit kan bijvoorbeeld per sector zijn. De AP doet dit door de gedragscodes te beoordelen en te bekijken of de gedragscodes Wbp-compliant zijn. De AP heeft daarnaast de taak om ontwikkelingen op technisch gebied in de gaten te houden. Door deze ontwikkelingen kunnen persoonsgegevens namelijk met hogere snelheid en in grote omvang verwerkt worden. Het laatste pad dat de AP bewandelt om haar doelstellingen te behalen is handhaving. Door middel van toezicht houden beoordeelt de AP of verantwoordelijke organisaties compliant aan de Wbp handelen. De AP is een zelfstandig orgaan. Dat wil zeggen dat de AP onafhankelijk van de overheid haar taken uitvoert. De

[44] MvT Wbp, p. 65.
[45] Artikel 8 sub b Wbp.
[46] CBP 2001, p. 15-17.

AP moet namelijk ook zorgen dat en beoordelen of overheidsorganen compliant aan de Wbp handelen. [47]

De FG moet worden ingesteld door de organisatie zelf. De FG houdt toezicht op *'de verwerking van persoonsgegevens door de verantwoordelijke die hem heeft benoemd*'. Als een organisatie een FG heeft ingesteld, dient deze dat te melden aan het AP. Organisaties zijn op grond van de Wbp niet verplicht om een FG in te stellen.[48] De FG houdt intern in de organisatie in de gaten of er compliant aan de Wbp wordt gehandeld en houdt dus toezicht op de verwerking van persoonsgegevens. Daarnaast is de FG met al zijn of haar kennis omtrent privacy het aanspreekpunt van de verantwoordelijke organisaties als het gaat om het beschermen van de persoonlijke levenssfeer van betrokkenen en de verwerking van persoonsgegevens. Indien er een deskundige FG is aangesteld in een organisatie, zal de AP meer terughoudend te werk gaan. De FG moet betrouwbaar zijn, onafhankelijk zijn en bekwaam zijn op het gebied van het verwerken van persoonsgegevens. Een FG hoeft niet aan de AP te melden als zij zich bezighoudt met verwerkingen.[49]

3.8 Sanctionering

Het CBP kon in sommige gevallen een boete opleggen van tienduizend gulden. Deze boete wordt alleen opgelegd als de verantwoordelijke niet aannemelijk kan maken dat het overtreden van de Wbp niet aan hem te wijten is. Het CBP hield met het bepalen van de hoogte van de boete rekening met de aard en de duur van de overtreding.[50] Sinds 1 januari 2016 heeft de AP een grotere boetebevoegdheid volgens haar boetebeleidsregels. De AP houdt met het opleggen van de boetes nog steeds rekening met de aard en duur van de overtreding, op grond van haar boetebeleidsregels. Ook moet de AP rekening houden met de impact van de overtreding op de bescherming van persoonsgegevens en van de persoonlijke levenssfeer van de betrokkenen.[51] De boete die nu maximaal opgelegd kan worden door de AP is €820.000.[52]

3.9 Conclusie en onderzoekspunten

Met de komst van de Wbp zijn er een talrijk aantal veranderingen op het gebied van privacy. De Wbp introduceert het CBP en de FG. Daarnaast heeft het CBP met de komst van de Wbp voor het eerst de kans gekregen om een bestuurlijke boete op te leggen aan organisaties, indien deze niet compliant aan de Wbp handelen. Het CBP heet nu het AP. Sinds 1 januari 2016 heeft de AP een grotere boetebevoegdheid. Om de eerste deelvraag te kunnen beantwoorden is er in dit hoofdstuk belangrijke materie besproken omtrent de Wbp. In de Wbp wordt niet in gegaan op het hanteren van een privacybeleid in organisaties. Wel wordt van organisaties verwacht dat deze compliant aan de Wbp handelen en wordt er gesproken over gedragscodes. Initiatief voor een gedragscode komt van (verantwoordelijke) organisatie zelf. Deze zijn op grond van de Wbp niet verplicht om een gedragscode vast te stellen. Een onderzoekspunt voortvloeiend uit bovenstaand hoofdstuk is of de regels die de Wbp geeft, momenteel nageleefd worden in het UMCG en in een privacybeleid op zijn genomen. Dit is van belang omdat op dit moment sprake is van een overgangsfase waarin de Wbp nog van toepassing is en de huidige situatie in kaart moet worden gebracht om te kunnen onderzoeken waar verbeterpunten zitten. Op deze manier kan er gekeken worden of de bepalingen van de Wbp goed geïmplementeerd zijn in de organisatie. Indien dit niet het geval is, kan er met de komst van de EPV winst worden behaald bij de implementatie van de nieuwe wet- en regelgeving binnen de afdeling P&O van het UMCG.

[47] Artikel 25 Wbp.
[48] Berkvens 2002, p. 97-98.
[49] CBP 2001, p. 17-18.
[50] Artikel 66-73 Wbp.
[51] Artikel 6.1 sub C Boetebeleidsregels AP 2016.
[52] Artikel 2 lid 2.2 Boetebeleidsregels AP 2016.

4. Europese Privacy Verordening

De theorie die hieronder beschreven wordt is gericht op de volgende deelvragen:
- *Wat is opgenomen in de nieuwe wetgeving (EPV) omtrent hanteren van privacybeleid?*
- *Wat zijn in theorie belangrijke verschillen tussen de huidige wetgeving en de nieuwe wetgeving omtrent het hebben van privacybeleid?*
- *Wat is er in de juridische literatuur bekend over de consequenties van de invoering van de EPV voor organisaties?*

4.1 Belangrijke begrippen

In artikel 4 van de EPV zelf worden enkele definities besproken. Veelal zijn de begrippen in de EPV overgenomen van de Wbp. Er zijn echter ook wijzigingen doorgevoerd in begrippen of begrippen hebben een nieuwe naam gekregen. Achtereenvolgens zullen de begrippen besproken worden die van belang zijn voor de afdeling P&O van het UMCG.

4.1.1 Persoonsgegevens

In de EPV is het begrip persoonsgegevens gedefinieerd als '*iedere informatie betreffende een betrokkene'*. In vergelijking met hetzelfde begrip in de Wbp is de definitie een stuk bondiger geworden.

4.1.2 Verwerking

De definitie van de 'verwerking van persoonsgegevens' heet in de EPV 'verwerking'. Het begrip is in de EPV gedefinieerd als '*een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens'*.

4.1.3 Bijzondere gegevens

In het voorgaande stuk gericht op de Wbp is te lezen dat deze een artikel heeft met betrekking tot bijzondere gegevens. Ook in de EPV is er een speciaal artikel, gericht op bijzondere persoonsgegevens. Het enige toegevoegde aan het artikel uit de Wbp is dat een genetisch gegeven ook een bijzonder gegeven is. In beginsel is het verwerken van bijzondere gegevens verboden. Enkele uitzonderingen op het verbod tot het verwerken van bijzondere gegevens staan vermeldt in hetzelfde artikel.

4.1.4 De betrokkene

Een betrokkene is volgens de EPV een geïdentificeerde of identificeerbare natuurlijke persoon. Als identificeerbaar wordt beschouwd '*een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon'*. Van belang is dus dat er sprake is van een natuurlijk persoon, die identificeerbaar is. Dit begrip is ten opzichte van de Wbp flink uitgebreid. Onder het begrip persoonsgegeven in de Wbp, wordt ingegaan op een natuurlijk persoon en de identificeerbaarheid hiervan (zie paragraaf 3.1.1).

4.1.5 De verwerkingsverantwoordelijke

De verantwoordelijke staat in de EPV beschreven als de '*verwerkingsverantwoordelijke'*. De definitie is overwegend hetzelfde gebleven als in de Wbp, hier is alleen aan toegevoegd dat als het doel, de voorwaarden en de middelen voor de verwerking worden vastgesteld bij Europese of nationale

wetgeving, hierin ook kan worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.

4.1.6 De verwerker

De verwerker wordt omschreven als '*de natuurlijke of rechtspersoon, de overheidsinstantie, de dienst of enig ander orgaan die, respectievelijk dat, ten behoeve van de voor de verwerking verantwoordelijke persoonsgegevens verwerkt'*. In de Wbp heet de verwerker de 'bewerker' en was het begrip veel bondiger.

4.1.7. Toestemming van de betrokkene

Toestemming van de betrokkene wordt in de EPV omschreven als '*elke vrije, specifieke, op informatie berustende en uitdrukkelijke wilsuiting waarmee de betrokkene, door middel van hetzij een verklaring hetzij een ondubbelzinnige actieve handeling aanvaardt dat hem betreffende persoonsgegevens worden verwerkt*'. Het begrip toestemming is in de Wbp soortgelijk. Er is echter aan de bepaling van de Wbp toegevoegd dat de toestemming ondubbelzinnig verstrekt moet zijn.

4.1.8. Pseudonimisering

Pseudonimisering is een nieuw begrip in de EPV. Het wordt omschreven *als 'het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld'*. Samengevat houdt dit begrip in dat de persoonsgegevens op zodanige wijze zijn verwerkt dat deze anoniem zijn geworden.

4.1.9 Inbreuk in verband met persoonsgegevens

De inbreuk in verband met persoonsgegevens is een nieuw begrip in de EPV. Het wordt omschreven als *'een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens'*.

4.1.10 Gegevens over gezondheid

Gegevens over gezondheid worden gedefinieerd als '*persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven*'. Dit spreekt voor zich.

4.1.11 Beperken van de verwerking

Het beperken van de verwerking is een nieuw recht die de betrokkene heeft. In de EPV staat het begrip omschreven als 'het markeren van opgeslagen persoonsgegevens met als doel de verwerking ervan in de toekomst te beperken'. Hier wordt verder op ingegaan in paragraaf 4.6. [53]

4.2 Historie

De EPV is de rechtsopvolger van de Wbp. In 2012 kwam de Europese Commissie met het voorstel voor een nieuwe verordening. Op 25 januari 2012 heeft de Commissie dan ook een pakket ingediend, waar dit voorstel in verwerkt was.[54] De bedoeling van de Commissie was om met dit voorstel de geldende Europese privacyregelgeving te vervangen, wat bestaat uit de *'Richtlijn Gegevensbescherming'* en het *'Kaderbesluit Gegevensbescherming voor politiële en justitiële samenwerking in strafzaken'*. Er is gekozen voor een verordening, aangezien deze na een

[53] Artikel 4 EPV.
[54] De Jong 2015, p. 6.

overgangstermijn rechtstreeks geldend is in alle lidstaten. Anders dan een richtlijn, hoeft een verordening dus niet geïmplementeerd te worden door de nationale wetgever in nationale wetgeving. In de EPV staat zelf omschreven wat de achterliggende gedachten zijn van de Europese wetgever met betrekking tot de privacyverordening. De wetgever geeft aan dat de snelle technologische ontwikkelingen zorgen voor nieuwe uitdagingen als het gaat om de bescherming van persoonsgegevens. De bedrijven en de overheid kunnen door deze ontwikkelingen flink gebruikmaken van persoonsgegevens. Er moet vertrouwen in de onlineomgeving gecreëerd worden, anders kunnen consumenten gaan twijfelen of zij wel online moeten kopen. Deze twijfels kunnen als gevolg hebben dat de ontwikkeling van de nieuwe technologieën vertraagd worden.[55]

4.3 Beginselen

De beginselen van de Wbp zijn grotendeels gelijk gebleven in de EPV. Er zijn wat kleine detailverschillen waarneembaar indien de EPV en de Wbp naast elkaar worden gelegd.[56] Er zijn twee aanpassingen binnen de hoofdbeginselen van de Wbp met de komst van de EPV. Het eerst element is transparantie. Dit houdt in dat bij het verwerken van persoonsgegevens een doorzichtige, open en eerlijke houding wordt verwacht van de verweringsverantwoordelijke. Transparantie heeft, met de komst van de EPV, een eigen plek in de wetgeving gekregen en is daarmee flink aangescherpt. Het tweede, toegevoegde element is de verantwoordingsplicht. De verwerkingsverantwoordelijke heeft een verantwoordingsplicht gekregen. Dit houdt in dat de degene die persoonsgegevens verwerkt verantwoording dient af te leggen aan de toezichthouder en aan betrokkenen over aard en doel van de gegevensverwerking.[57]

4.4 Reikwijdte

Net als in de Wbp wordt de reikwijdte van de EPV ten eerste bepaald door de begrippen ‘persoonsgegevens’ en ‘verwerken’. De EPV is namelijk alleen geldend als er sprake is van een persoonsgegeven en dit persoonsgegeven verwerkt wordt. Daarnaast wordt de reikwijdte van de EPV beschreven in de beginartikelen van de EPV zelf. Het materiële toepassingsgebied houdt in dat de verordening van toepassing is op de geheel of gedeeltelijk geautomatiseerde en de niet-geautomatiseerde verwerking van persoonsgegevens, die in een bestand zijn opgenomen of die zijn bestemd daarin te worden opgenomen. Ook bevat de EPV een territoriaal toepassingsgebied. De EPV is namelijk van toepassing op de verwerking van persoonsgegevens in het kader van de activiteiten van een vestiging van een verwerkingsverantwoordelijke of een verwerker in de Europese Unie. Tevens is de EPV in twee gevallen van toepassing als de verwerkingsverantwoordelijke niet in de Europese Unie woont, maar de betrokkene wel. De twee gevallen zijn; het aanbieden van goederen of diensten aan deze betrokkenen of het observeren van het gedrag van de betrokkenen.[58]

4.5 Rechtmatigheid verwerking

Uit paragraaf 4.3 blijkt dat persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is. De verwerking is alleen rechtmatig indien en voor zover aan ten minste één van de volgende voorwaarden is voldaan:

- De betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor één of meer specifieke doeleinden.
- De verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is.
- De verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die de verwerkingsverantwoordelijke heeft.

[55] Wetsvoorstel EPV 25 januari 2012, p. 1-2.
[56] De Jong 2015, p. 9.
[57] Artikel 5 lid 1 en lid 2 EPV.
[58] Artikel 2 en 3 EPV.

- De verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een ander natuurlijke persoon te beschermen.
- De verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak van openbaar gezag die de verwerkingsverantwoordelijke heeft.
- De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, tenzij de belangen, de grondrechten en de fundamentele vrijheden van de betrokkene zwaarder wegen dan die belangen.[59]

4.6 Rechten van betrokkene

Met de komst van de EPV heeft de betrokkene aanzienlijk meer rechten gekregen, of de rechten zijn in een apart artikel opgenomen. Hieruit kan worden afgeleid dat de wetgever de belangen van de betrokkene hoog in het vaandel heeft staan.

Het recht van de betrokkene om in bezwaar te gaan tegen de verwerking van zijn of haar persoonsgegevens is overgenomen in de EPV. De betrokkene heeft het recht om in bezwaar te gaan tegen de gegevensverwerking indien de verwerkingsverantwoordelijke de persoonsgegevens verwerkt omdat; de verwerking noodzakelijk is om de vitale belangen van de betrokkene te beschermen, de verwerking noodzakelijk is voor de vervulling van een taak uit algemeen belang of voor de uitoefening van openbaar gezag, als de verantwoordelijke hiermee is belast. Daarnaast kan de betrokkene bezwaar maken tegen de verwerking indien de gegevens verwerkt worden omdat dit noodzakelijk is voor de behartiging van de gerechtvaardigde belangen van de verantwoordelijke. Bij gegrond bezwaar worden de persoonsgegevens niet langer voor de in het bezwaar omschreven doeleinden gebruikt of anderszins verwerkt.[60]

Het recht op rectificatie van de betrokkene betreffende onjuiste of incomplete persoonsgegevensverwerking door de verwerkingsverantwoordelijke en het recht op toegang tot alle informatie omtrent de persoonsgegevens van de betrokkene hebben in de EPV, anders dan in de Wbp, een eigen artikel gekregen. Het recht op toegang houdt in dat de betrokkene te allen tijde het recht heeft op alle informatie met betrekking tot zijn persoonsgegevens, bijvoorbeeld of zijn persoonsgegevens wel of niet verwerkt worden. De betrokkene heeft daarnaast recht op beperking van de verwerking. De betrokkene heeft het recht van de verwerkingsverantwoordelijke de beperking van de verwerking te verkrijgen indien de verwerkte gegevens onjuist zijn, onrechtmatig verwerkt worden, de verwerkingsverantwoordelijke heeft de persoonsgegevens niet meer nodig voor de verwerkingsdoeleinden of indien de betrokkene in bezwaar is gegaan tegen de verwerking.[61]

Een nieuw recht voor de betrokkene is het gecombineerde recht op wissing en afscherming van de persoonsgegevens. Betrokkenen hebben het recht op wissing en afscherming indien de verantwoordelijke organisatie de gegevens niet meer nodig heeft in verband met de doeleinden waarvoor zij werden verzameld of anderszins verwerkt, indien hij of zij de toestemming die gegeven is voor de verwerking van de gegevens intrekt, indien de persoonsgegevens onrechtmatig zijn verwerkt en/of indien de gegevens op grond van een wettelijke verplichting moeten worden gewist. Ook kan de betrokkene gebruik maken van zijn recht op wissing en afscherming door bezwaar aan te tekenen. Indien de verwerking van de gegevens op andere gronden niet compliant aan de EPV is, heeft de betrokkene altijd het recht op wissing en afscherming.[62] Met de komst van de EPV dienen de persoonsgegevensgegevens niet alleen uit het bestand van de verwerkingsverantwoordelijke gewist te worden, maar wanneer de verwerkingsverantwoordelijke de persoonsgegevens openbaar heeft gemaakt en verplicht is de persoonsgegevens te wissen, moet de verwerkingsverantwoordelijke rekening houdend met de beschikbare technologie en de uitvoeringskosten, redelijke maatregelen,

[59] Artikel 6 EPV.
[60] Artikel 21 EPV.
[61] Artikel 16 EPV.
[62] Artikel 15-22 EPV.

waaronder technische maatregelen, om verwerkingsverantwoordelijken die de persoonsgegevens van deze betrokkene (ook) verwerken, ervan op de hoogte te stellen dat de betrokkene de verwerkingsverantwoordelijken heeft verzocht om iedere koppeling naar, of kopie of reproductie van die persoonsgegevens te wissen.[63]

Tevens is een nieuw recht het recht van gegevensoverdraagbaarheid. Dit wordt ook wel het recht van dataportabiliteit genoemd. De betrokkene krijgt hiermee het recht om zijn persoonsgegevens mee te nemen van de ene naar de andere verwerkingsverantwoordelijke. Dit kan alleen wanneer persoonsgegevens elektronisch en in een gestructureerd en algemeen gebruikt format zijn verwerkt.[64]

4.7 Verplichtingen van de verantwoordelijke

Tegenover de rechten van de betrokkenen staan de verplichtingen van de verweringsverantwoordelijke. De organisatie is verplicht om alle rechten van de betrokkenen te faciliteren.[65] Alleen indien de verantwoordelijke zich houdt aan de bepalingen van de EPV en daarmee compliant aan de EPV handelt, kunnen persoonsgegevens rechtmatig verwerkt worden. Het doel van deze verplichtingen is dat de verwerking transparant en eerlijk is naar de betrokkenen en toezichthouders toe. Om als betrokkene rechten uit te kunnen oefenen, moet je wel weten welke gegevens worden verwerkt en met welk doel. Indien betrokkenen niet weten welke gegevens worden verwerkt, zullen zij onwetend zijn en daarmee niet in staat om hun rechten uit te kunnen oefenen. In de EPV worden de verplichtingen van de verantwoordelijke uitgebreid, om zo meer bescherming te kunnen garanderen aan de betrokkenen.[66]

De verantwoordelijke heeft een informatieplicht. Dit houdt in dat de verwerkingsverantwoordelijke verplicht is de betrokkene van de volgende informatie te voorzien, namelijk; haar contactgegevens, het doel van de gegevensverwerking, de bewaartermijn en de rechten die de betrokkene heeft.[67]

De verwerkingsverantwoordelijke moet, met de komst van de nieuwe verordening, actief (privacy)beleid gaan voeren en maatregelen treffen voor verplichtingen die zij gaat krijgen. Daarnaast dient de verantwoordelijke ‘privacy bij default’ en ‘privacy by design’ toe te passen. Deze twee termen houden in dat de verantwoordelijke er zorg voor moet dragen dat er passende technische en organisatorische maatregelen en procedures worden gehanteerd, zodat de verwerking van de persoonsgegevens compliant aan de EPV is.[68] Hier wordt verder op ingegaan in paragraaf 4.10.

Daarnaast moet de verantwoordelijke er oog voor houden dat de rechten van de betrokkenen zo goed mogelijk gewaarborgd blijven. Net zoals in de Wbp geregeld is, dient de verantwoordelijke te allen tijde te zorgen voor passende beveiliging.[69] De EPV eist dat de verantwoordelijke organisatie de risico’s in kaart brengt en daarop passende technische en organisatorische maatregelen met betrekking tot de beveiliging van de persoonsgegevens treft.[70] Tevens moet de organisatie zorgen dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is. Hiervoor dient de verwerkingsverantwoordelijke termijnen vast te stellen voor het wissen van gegevens of voor een periodieke toetsing ervan.[71]

[63] Artikel 17 lid 2 EPV.
[64] De Jong 2015, p. 11.
[65] Artikel 12 lid 2 EPV.
[66] De Jong 2015, p. 11.
[67] Artikel 14 EPV.
[68] Artikel 24-25 EPV.
[69] Artikel 30 EPV.
[70] Artikel 23 EPV.
[71] Overweging 39 EPV.

De verwerkingsverantwoordelijke moet regelingen treffen om de betrokkene in staat te stellen om het recht van bezwaar uit te oefenen. Het recht van bezwaar moet ook langs de elektronische weg kunnen worden uitgeoefend. De verantwoordelijke moet onverwijld en ten laatste binnen een maand op het verzoek van de betrokkene reageren.[72]

4.8 Gegevensverwerking werknemers

Het onderzoek is toegespitst op de afdeling P&O. Deze personeelsafdeling verwerkt persoonsgegevens van werknemers. Elke werknemer heeft zijn eigen dossier. In de EPV is een apart artikel opgenomen over de verwerking van persoonsgegevens in het kader van de arbeidsverhouding. Dit artikel machtigt de lidstaten specifieke wetgeving aan te nemen voor de verwerking van persoonsgegevens in het kader van de arbeidsverhouding. Dit is enigszins opvallend te noemen, omdat er op deze manier geen volledig uniforme privacywetgeving op het gebied van het arbeidsrecht gerealiseerd wordt, terwijl uniformiteit in de privacywetgeving binnen de lidstaten van de Europese Unie wel als een belangrijke doelstelling van de EPV wordt genoemd. Er is hierdoor enigszins beleidsvrijheid toegekend aan de lidstaten.[73]

De specifieke wetgeving die eventueel door de lidstaten opgesteld mag worden in het kader van de arbeidsverhouding moeten wel binnen de grenzen van de EPV vallen. In een brief van de Staatssecretaris van Veiligheid en Justitie aan de Tweede Kamer wordt aangenomen dat de bepalingen van de verordening leidend zijn als minimumniveau van bescherming voor verwerking in de arbeidsrelatie. Niet uitgesloten wordt dat een hoger beschermingsniveau kan worden vastgesteld voor het verzamelen, gebruiken en verstrekken van persoonsgegevens in de context van de arbeidsverhouding.[74]

4.8.1. Toestemming van de werknemer

Zoals al eerder aangehaald in dit onderzoek kan een verwerkingsverantwoordelijke persoonsgegevens alleen rechtmatig verwerken indien aan één van de voorwaarden hiervoor wordt voldaan (zie paragraaf 4.5). De verantwoordelijke organisatie mag alleen persoonsgegevens verwerken indien de EPV haar hiervoor mogelijkheid biedt. Eén van deze rechtsgrondslagen is dat het verwerken van persoonsgegevens door de verantwoordelijke organisatie mag, indien de betrokkene daarvoor toestemming heeft gegeven.[75] Indien er sprake van een arbeidsrelatie is, ligt dit anders. In de EPV is namelijk opgenomen dat toestemming van de betrokkene geen goede voorwaarde is voor de verwerking van persoonsgegevens indien er sprake is van ‘wanverhouding’ in de relatie tussen de verwerkingsverantwoordelijke en de betrokkene.[76] Omdat er in een arbeidsverhouding enige hiërarchie bestaat tussen werkgever en werknemer, kan er sprake zijn van zo’n wanverhouding. Er is namelijk sprake van macht bij de werkgever.

Aangenomen kan worden dat de bepaling in de EPV hetzelfde geïnterpreteerd moet worden als bij de Wbp, omdat het begrip ‘toestemming van de betrokkene’ dezelfde elementen bevat waaraan voldaan moet zijn om te spreken van toestemming voor de verwerking.[77] Het dus discutabel om als verwerkingsverantwoordelijke toestemming van de werknemer te gebruiken als voorwaarde voor het verwerken van zijn of haar persoonsgegevens. Op de afdeling P&O zullen veelal persoonsgevens verwerkt worden omdat de verwerking noodzakelijk is voor de uitvoering van de arbeidsovereenkomst waarbij de medewerker partij is. Ook is de verwerking soms noodzakelijk omdat er door het UMCG voldaan moet worden aan een wettelijke verplichting, zoals de sociale verzekeringswetgeving.

[72] Overweging 59 EPV.
[73] Artikel 88 EPV.
[74] *Kamerstuk II* 2014, 32 761, nr. 60, p. 4.
[75] Artikel 6 lid 1 sub a EPV.
[76] Overweging 43 EPV.
[77] Overweging 34 EPV.

4.8.2. Zieke werknemers

De afdeling P&O zal meer dan eens te maken krijgen met ziekteverzuim. Hierdoor zullen misschien gegevens moeten worden verwerkt omtrent het ziekteverzuim van een werknemer. Het is belangrijk om in het toekomstige privacybeleid op te nemen hoe deze gegevens verwerkt worden en door wie. Het is namelijk niet zonder meer toegestaan om persoonsgegevens omtrent de zieke werknemer te verwerken. Zoals al eerder besproken vallen medische gegevens van betrokkenen onder de zogenaamde 'bijzondere persoonsgegevens'. Deze persoonsgegevens krijgen extra bescherming op grond van de EPV. Niet alle gegevens over ziekte(verzuim) van werknemers mogen zomaar door werkgevers verwerkt worden. De AP heeft op 21 april 2016 een rapport gepubliceerd waarin beschreven wordt hoe zij als toezichthoudend orgaan haar taken uitvoert met betrekking tot situaties van gegevensverwerking, indien er sprake is van ziekte bij een werknemer. Dit rapport vervangt het eerdere rapport uit 2008. Omdat de EPV nog niet in werking is getreden, worden in het rapport artikelen gebruikt uit de Wbp. Wel geeft de AP in haar voorwoord aan dat er op voorhand rekening is gehouden met nieuwe wetgeving, de EPV. Enkele belangrijke beleidsregels worden weergegeven en omschreven in bijlage 2 vanaf pagina 77.

4.9 Privacybeleid

In de EPV is voor het eerst de verplichting voor organisaties opgenomen om een intern beleid omtrent het verwerken van gegevens te gaan hanteren. De verplichting tot het voeren van een privacybeleid is niet eerder geïntroduceerd in privacywetgeving. Dit privacybeleid moet compliant zijn aan de bepalingen van de EPV.

Het interne gevoerde privacybeleid dient aan enkele voorwaarden uit de EPV te voldoen. Allereerst dient het privacybeleid van de verantwoordelijke transparant en eenvoudig toegankelijk te zijn. Hierbij moet in acht genomen worden dat het privacybeleid leesbaar is voor de betrokkenen waarvan de gegevens worden verwerkt. Er moet rekening gehouden worden met de eventuele verschillende leesniveaus van betrokkenen. De verantwoordelijke verschaft de betrokkene in begrijpelijke vorm alle informatie en mededelingen over de verwerking van persoonsgegevens, waarbij duidelijke en eenvoudige, aan de betrokkene aangepaste taal wordt gebruikt. De nadruk in dit artikel van de EPV wordt gelegd op informatie die specifiek voor kinderen is opgesteld.[78] Het toezicht op de naleving van het interne privacybeleid wordt uitgevoerd door de FG.[79]

Om de persoonsgegevens van de betrokkenen in verband met de verwerking hiervan door verantwoordelijken voldoende bescherming te bieden, moet een organisatie op grond van de EPV voldoende passende technische en organisatorische maatregelen treffen.[80] De organisatie moet zorg dragen dat er aan de bepalingen van de EPV wordt voldaan zodat zij compliant aan de EPV handelt. De verantwoordelijke organisatie wordt geacht dit te doen door intern beleid vast te stellen omtrent de verwerking van persoonsgegevens van betrokkenen.[81] De organisatie dient de beginselen; privacy by design en privacy by default hierbij toe te passen.

4.10 Privacy by design en privacy by default

Extra aandacht verdienen de twee nieuwe termen; privacy by design en privacy by default. De begrippen zijn niet letterlijk genoemd in de EPV, maar komen hier inhoudelijk wel in terug.[82] Allereerst is het belangrijk om het verschil tussen deze twee begrippen noemen. Met privacy by design wordt bedoelt dat de privacy gelijk vanaf het begin van gewaarborgd dient te worden.

Hoewel een eenduidige definitie ontbreekt wordt hiermee vaak bedoeld dat al bij het ontwerpen en

[78] Artikel 11 EPV.
[79] Artikel 39 EPV.
[80] Artikel 24 EPV.
[81] Artikel 22 EPV.
[82] Artikel 24-25 EPV.

de toepassing van technologie rekening moet worden gehouden met de noodzaak van privacybescherming.[83]

Volgens deskundige Van Lieshout is er sprake van privacy by design indien;
- De bescherming van de privacy van personen over wie gegevens verzameld worden (bijvoorbeeld consumenten) al bij het (vroegste) ontwerp van een systeem wordt meegenomen.
- Er gebruik wordt gemaakt van organisatorische maatregelen om toegang tot en omgang met persoonsgegevens te regelen volgens bepaalde afspraken en voorschriften.
- Er gebruik wordt gemaakt van technische maatregelen zoals versleuteling om toegang tot en omgang met persoonsgegevens af te schermen of te verhinderen.[84]

Met privacy by default wordt bedoeld dat er een maximaal haalbaar privacyhandhaving moet worden nagestreefd en aangeboden door organisaties, waardoor de maximale bescherming van de persoonsgegevens van de betrokkene wordt gewaarborgd. Opgemerkt dient te worden dat privacy by design en privacy by default dusdanig samenhangen dat deze niet los van elkaar moeten worden gezien. Vanaf de beginfase moet er volgens privacy de term privacy by design en privacy by default rekening gehouden worden met privacy. In elke stap dient gegevensbescherming worden meegenomen en wel op het maximaal haalbaar niveau. De ontwerpfase dient geleid te worden door privacy principes, zoals een Privacy Impact Assessment (zie paragraaf 4.11). Daarnaast moet er met de keus van technologie rekening gehouden worden met privacy. De keus voor een bepaald instrument moet bijvoorbeeld mede gemaakt worden op grond van de transparantie en bescherming die dit instrument voor de betrokkene biedt. Tevens dient de organisatie organisatorische instrumenten in te zetten, zoals een FG, en de fysieke ruimtes dienen privacy recht te doen.[85]

4.11 Privacy Impact Assessment

Een Privacy Impact Assessment (PIA) is een methode van voorafgaand onderzoek, die op een systematische en gestructureerde manier helpt om privacyrisico's inzichtelijk te maken. In de EPV wordt dit een gegevensbeschermingseffectbeoordeling genoemd. Verantwoordelijke organisaties die gegevens verwerken die gezien hun aard, reikwijdte of doeleinden risico's opleveren voor de betrokkene dienen een beoordeling uit te voeren van het effect van de beoogde verwerkingen op de bescherming van persoonsgegevens.[86] Een PIA is een voorbeeld van zo'n beoordeling. Door middel van een PIA kunnen vooraf de risico's in kaart worden gebracht en verkleind worden. De PIA is in de EPV verplicht gesteld voor organisaties.[87]

4.12 Register van de verwerkingsactiviteiten

Verantwoordelijken zijn verplicht om alle documenten omtrent de verwerking van persoonsgegevens te bewaren die onder hun verantwoordelijkheid hebben plaatsgevonden in een Register van de verwerkingsactiviteiten. De documentatie is volgens de EPV correct indien deze de volgende gegevens bevat:

1. De naam en contactgegevens van de verantwoordelijke.
2. De naam en contactgegevens van de (eventuele) verwerker.
3. De naam en contactgegevens van de FG.
4. De doelen van de verwerking.
5. Indien de gegevens verwerkt worden voor gerechtvaardigd belang van de verantwoordelijke, de redenen hiervan en de noodzakelijkheid.

[83] Van Lieshout 2012, p. 15.
[84] Van Lieshout 2012, p. 2-3.
[85] Van Lieshout 2012, p. 3.
[86] Artikel 35 EPV.
[87] Van Lieshout 2012, p. 38.

6. De beschrijving van de categorieën betrokkenen en persoonsgegevens.

7. De termijnen waarbinnen (de categorieën) gegevens moeten worden gewist.

8. Een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.[88]

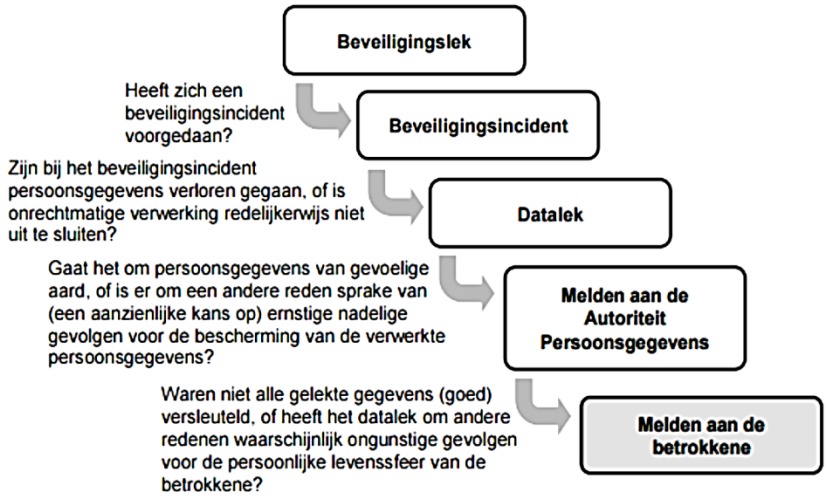
4.13 Incidenten

Een incident op het gebied van privacy kan ruim omschreven worden. Gedacht kan worden aan een klacht omtrent de gegevensverwerking van persoonsgegevens of een interne melding dat er iets in een procedure omtrent gegevensverwerking schort. Het meest bekende incident is de zogenaamde datalek. Dit is een (omvangrijke) inbreuk op het registratiesysteem waarin de gegevens opgeslagen staan, waardoor deze niet meer goed beveiligd is. Een voorbeeld van een datalek is als het registratiesysteem gehackt wordt. Sinds 1 januari 2016 geldt er de 'Meldplicht datalekken'.[89]

De AP heeft beleidsregels opgesteld voor organisaties, zodat zij weten wanneer er sprake is van een datalek en hoe zij hiermee om moeten gaan. Indien er sprake is van een inbreuk, dient de verantwoordelijke organisatie in ieder geval binnen 72 uur nadat zij achter het lek is gekomen, de toezichthoudende autoriteit op te hoogte te brengen van de inbreuk. Als dit niet binnen 72 uur wordt gedaan, dient gemotiveerd te worden wat de reden hiervan is. De verantwoordelijke organisatie moet aan de AP melden wat de aard van de inbreuk is, op welke categorieën dit is, om hoeveel persoonsgegevens van betrokkenen het gaat, wat de contactgegevens van de FG zijn, wat de gevolgen van de inbreuk zijn en welke maatregelen de verantwoordelijke aanbeveelt om de gevolgen van de inbreuk zo klein mogelijk te houden en aan te pakken. Daarnaast is de verantwoordelijke organisatie verplicht om alle inbreuken op het gebied van privacy uitgebreid te registreren en documenteren. De toezichthouder kan dan aan de hand van de documentatie controleren of de verantwoordelijke organisatie zich houdt aan de bepalingen van de EPV.[90]

Tevens dient de verantwoordelijke organisatie, na het op de hoogte stellen van de toezichthouder, de betrokkenen soms te informeren over de inbreuk. Dit hoeft alleen als het lek (waarschijnlijk) negatief kan uitvallen voor de betrokkenen. In de melding aan de betrokkene dient in ieder geval dezelfde informatie te staan als in de melding aan de toezichthouder. De melding aan de betrokkene hoeft niet voor zover de verantwoordelijke organisatie aan de toezichthouder laat zien dat zij voldoende passende maatregelen heeft genomen om de gegevens waar inbreuk op is gemaakt te beschermen. Dit kan bijvoorbeeld door de gegevens onbegrijpelijk te maken voor degene die de gegevens onbedoeld in handen heeft. Als de toezichthouder oordeelt dat de inbreuk gemeld dient te worden aan de betrokkene, is de verantwoordelijke organisatie verplicht dit te doen, ongeacht of deze vindt dat negatieve gevolgen waarschijnlijk of onwaarschijnlijk zijn.[91]

[88] Artikel 30 EPV.
[89] Beleidsregels AP Meldplicht datalekken 2015, p. 4-5
[90] Artikel 33 lid 5 EPV.
[91] Artikel 32 EPV.



Figuur melden incidenten AP

4.14 Handhaving

Op grond van de EPV oefent elke toezichthouder op het grondgebied van haar lidstaat de bevoegdheden uit die haar overeenkomstig deze verordening zijn toegekend.[92] Er moet sprake zijn van een goed geregelde onderlinge samenwerking tussen de toezichthouders van de 28 lidstaten. Bij de uitvoering van een verordening is een centrale toezichthouder eigenlijk voor de hand liggend, omdat de handhaving en het toezichthouden uniform dient plaats te vinden. In de 28 lidstaten wonen ongeveer 500 miljoen mensen. Eén uniforme toezichthouder voor al deze burgers is met zo'n uitgebreide, strenge verordening eigenlijk onmogelijk. Met oog daarop is besloten dat de nationale toezichthouders hun plek behouden. De toezichthouders dienen onafhankelijk en consequent te werk te gaan. Onze nationale toezichthouder is de AP.[93]

4.15 Sanctionering

Indien verantwoordelijke organisaties zich niet houden aan de bepalingen van de EPV zijn er verschillende administratieve sancties die opgelegd kunnen worden. De sanctiebevoegdheden van de nationale toezichthouder zijn met komst van de EPV flink uitgebreid. De AP heeft bevoegdheid gekregen om bestuurlijke boetes op te leggen, variërend van €250.000 tot €1.000.000, of de boete kan 0,5% tot 2% van de jaaromzet van de verantwoordelijke organisatie bedragen. De Commissie heeft ervoor gekozen om de boetebedragen te regelen in de EPV, waardoor deze rechtstreeks werkend zijn in de lidstaten van de Europese Unie. De Commissie heeft dit gedaan zodat er onderlinge verschillen in sanctionering zoveel mogelijk uitblijven. De toezichthouders hebben hierin niet veel beleidsvrijheid. De lidstaten dienen voldoende maatregelen te treffen om toepassing van de sancties te garanderen. De vastgestelde sancties moeten volgens de EPV doeltreffend, evenredig en afschrikkend zijn.[94]

De aard, de ernst, de duur van de inbreuk op de EPV en eventuele opzettelijkheid of nalatigheid moet worden meegenomen in de bepaling van het bedrag van de administratieve geldboete. Ook dient hierin meegenomen te worden of de verwerkingsverantwoordelijke al eerder inbreuk op de bepalingen van de EPV heeft gepleegd en of de organisatie de eisen aan de technische en organisatorische maatregelen en procedures van privacy by design en default heeft toegepast. Daarnaast wordt de mate waarin er door de verwerkingsverantwoordelijke met de toezichthoudende

[92] Artikel 51 EPV.
[93] De Jong 2015, p. 13.
[94] De Jong 2015, p. 14.

autoriteit is samengewerkt om de inbreuk te verhelpen meegenomen. Voor het niet hanteren van een privacybeleid kan de organisatie een boete uit de hoogste categorie krijgen. [95]

4.16 Conclusie en onderzoekspunten

Met de komst van de EPV zijn er een talrijk aantal nieuwe verplichtingen voor organisaties. Zo is een FG voor grote organisaties verplicht geworden. Daarnaast moeten de organisaties zorgen voor een privacybeleid, dat ertoe moet leiden dat de organisatie compliant aan de bepalingen van de EPV handelt. Onderzocht moet worden of de afdeling P&O van het UMCG een privacybeleid hanteert. Daarnaast moet onderzocht worden of dit privacybeleid voldoet aan de bepalingen van de EPV. De verplichtingen die de afdeling P&O heeft op grond van de EPV dienen opgenomen te zijn. Daarnaast moeten de rechten die een medewerker als betrokkene heeft in het privacybeleid staan en gefaciliteerd zijn. Tevens moet onderzocht worden of het eventuele privacyreglement aan privacy by design en privacy by default voldoet, of de incidenten met betrekking tot gegevensbescherming aan bod komen en of de organisatie de persoonsgegevens niet langer worden bewaard dan noodzakelijk is.

[95] Artikel 83-84 EPV.

5. Totstandkoming privacybeleid

De bepalingen van de EPV die belangrijk zijn voor het privacybeleid op de afdeling P&O zijn in hoofdstuk 5 doorgenomen. Om een goed werkend privacybeleid op te kunnen stellen, moet er gekeken worden wat er in de literatuur bekend is over het opstellen van een privacybeleid. Hierdoor kunnen fouten voorkomen worden. De volgende theorie is gericht op de volgende deelvraag:
- *Wat is er in de (juridische) literatuur bekend omtrent het opstellen van (privacy)beleid?*

5.1 Stakeholders

Voordat er een begin gemaakt kan worden met het schrijven van het (privacy)beleid, dient er eerst geïnventariseerd te worden welke partijen, direct of indirect, bij het opstellen van het beleidsplan betrokken zijn.[96] De verschillende partijen worden ook wel stakeholders of actoren genoemd. Belangrijk is dat met het schrijven van het beleidsplan oog op de stakeholders gehouden wordt. Volgens de EPV dient de verantwoordelijke een beleid op te stellen dat eenvoudig toegankelijk is en de informatie dient verschaft te worden in duidelijke, eenvoudige en op de betrokkene afgestemde taalgebruik.[97]

Indien er een privacybeleid wordt opgesteld, gericht op de afdeling P&O, zullen de volgende partijen als stakeholders figureren:

- De opdrachtgever: De opdrachtgever voor het opstellen van het beleidsplan is een belangrijke, direct betrokken partij. De opdrachtgever zorgt namelijk voor het budget om het beleidsplan te realiseren. Voor het opstellen van het privacybeleid met betrekking tot de afdeling P&O is het hoofd van de afdeling Juridische Zaken de opdrachtgever.

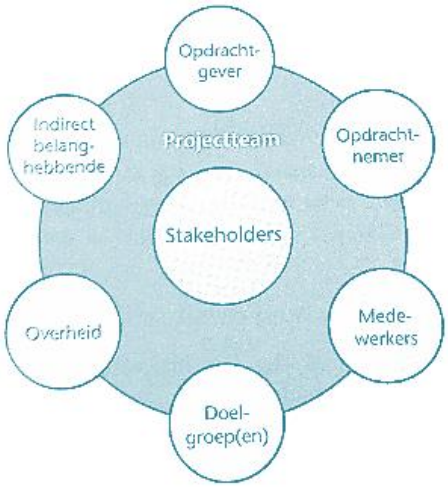
- De opdrachtnemer: De opdrachtnemer zorgt voor het opstellen en is verantwoordelijke voor uitvoering van het beleid. In dit onderzoek is de opdrachtnemer de 'Privacy werkorganisatie' van het UMCG.

- De overheid: De overheid is een belangrijke partij bij het opstellen van het privacybeleid. Bij het schrijven van het privacybeleid dient rekening gehouden te worden met de wetgeving, de EPV, en de handhaving hiervan, de AP.

- De medewerkers: De medewerkers zijn met het schrijven van het privacybeleid een belangrijke groep. Voor hen wordt het beleidsplan opgesteld en zij zullen het beleid uitvoeren. Omdat het privacybeleid is toegespitst op de afdeling P&O, zijn zij ook belanghebbenden.

- De belanghebbenden: De belanghebbenden zijn de betrokken personen waarvan de persoonsgegevens worden verwerkt. Het privacybeleid is gericht op de afdeling P&O. Daarom zijn de medewerkers ook de personen waarvan de persoonsgegevens worden verwerkt.

- De doelgroep: De doelgroep is de groep mensen voor wie het privacybeleid geformuleerd wordt. Dit zijn in het geval van het privacybeleid voor de afdeling P&O, de medewerkers, de Privacy werkorganisatie en de afdeling Juridische Zaken.



Aangezien het privacybeleid is gericht op de afdeling P&O, overlappen enkele partijen elkaar.[98]

[96] Grit 2009, p. 18.
[97] Artikel 12 EPV.
[98] Grit 2009, p. 18.

5.2 Competenties beleidsschrijver

Een schrijver van beleid moet over bepaalde specifieke eigenschappen beschikken om een goed beleidsplan te kunnen opstellen. Allereerst is het belangrijk dat de beleidsschrijver kennis heeft van het terrein waar het beleid betrekking op heeft.[99] De beleidsschrijver van het UMCG zal kennis moeten hebben van het recht en van privacy. Daarnaast dient de beleidsschrijver een project kunnen leiden. Het beleidsplan moet namelijk met inachtneming van de planning en begroting geschreven worden. Een beleidsschrijver moet logisch kunnen redeneren en zijn keuzes helder kunnen verklaren. Tevens moet de schrijver probleemoplossend kunnen werken. De verantwoordelijke organisatie moet op de beleidsschrijver kunnen bouwen. Daarom wordt er van de beleidsmedewerker verwacht dat deze integer is.

5.3 Stappenplan

Indien er een privacybeleid opgesteld moet worden, is het belangrijk om te weten waar je als organisatie moet beginnen. Hierdoor is de kans aanzienlijk kleiner dat er belangrijke informatie over het hoofd wordt gezien voor of tijdens het opstellen van het privacybeleid. In deze paragraaf worden de eerste stappen besproken van de totstandkoming van een privacybeleid:

1. Inventariseer de huidige situatie.
2. Analyseer de huidige situatie.
3. Bepaalt het beleid.
4. Definieer projecten en maatregelen.
5. Schrijft een (concept) beleidsplan.
6. Rond het beleidsplan af.
7. Voer het beleidsplan uit.[100]

Alleen de stappen één en twee zullen uitgewerkt worden, omdat het onderzoek niet verder gaat dan die stappen. Het beleid zal door de organisatie zelf opgesteld worden naar aanleiding van het onderzoek. Stap twee, het analyseren van de huidige situatie, wordt gedaan na het praktijkgedeelte.

5.3.1. Inventariseer de huidige situatie

Allereerst is het van belang om informatie omtrent het beleidsterrein waarop het beleidsplan betrekking heeft te verzamelen. Er moet informatie verzameld worden over:

1. Het huidige beleid: het eventuele huidige privacybeleid van de afdeling P&O zal onderzocht worden in het praktijkgedeelte van dit onderzoek.
2. Het algemene beleid: indien er een algemeen privacybeleid is voor het gehele UMCG zal deze onderzocht worden in het praktijkgedeelte van dit onderzoek.
3. Relevante feiten: de relevante feiten zijn al behandeld in hoofdstuk 5. Europese Privacy Verordening.
5. De betrokkenen: wie de betrokkenen zijn is al onderzocht, namelijk in paragraaf 1.3 en 1.4.
6. De problemen: de problemen zijn in dit onderzoek al behandeld, namelijk in paragraaf 1.1.[101]

Uiteindelijk zal er een tactisch beleidsplan opgesteld worden. Dit is een beleidsplan gericht op een bepaald beleidsterrein. Het privacybeleid van het onderzoek is toegespitst op de afdeling P&O en heeft te maken met specifieke nieuwe privacyverordening.

Daarnaast moet bepaald worden welke hulpmiddelen gebruikt kunnen worden voor het onderzoek. Een hulpmiddel om het huidige beleid te analyseren is de SWOT-analyse. De SWOT-analyse bestaat uit twee soorten analyses, namelijk; de interne en externe analyse. Intern wordt er gekeken naar de sterke punten (Strengths) en de zwakke punten (Weaknesses) op het gebied van privacybeleid bij de afdeling P&O van het UMCG. Extern wordt er gekeken naar mogelijkheden en kansen die er zijn

[99] Grit 2009, p. 19-20.
[100] Grit 2009, p. 24.
[101] Grit 2009, p. 37.

(Oppertunities) en naar bedreigingen (Threats). De SWOT-analyse kan uitgevoerd worden na afronding van dit onderzoek, omdat dan duidelijk is wat het eventuele huidige privacybeleid van de afdeling P&O van het UMCG is. Voordat dit bepaald is, kan niet worden uitgezocht wat de zwakke en sterke punten zijn en welke kansen of bedreigingen de EPV de afdeling biedt.[102]

De factoren- en actorenanalyse zijn al uitgevoerd in dit onderzoek. In de factorenanalyse wordt onderzocht welke omstandigheden en ontwikkelingen van invloed zijn op het beleidsterrein van het beleid. In dit onderzoek zijn (verschillen tussen) de Wbp en de opkomst van de EPV zulke factoren. De actoren zijn in het begin van dit onderzoek al uitgezocht in paragraaf 1.3 en 1.4.

Voor het onderzoek is van belang om te weten wat de visie en missie zijn van het UMCG, en dan vooral van de afdeling Juridische Zaken. Daarnaast moeten de organisatiedoelen en de strategie die de afdeling Juridische Zaken gebruikt om haar doeleinden te bereiken in kaart gebracht worden. Ook moet bepaald worden in welk ontwikkelingsstadium het de afdeling Juridische Zaken en de afdeling P&O zich bevinden. De visie en missie van het UMCG met betrekking tot de verwerking van persoonsgegevens is het compliance handelen aan de EPV.

5.4 Conclusie en onderzoekspunten

In dit hoofdstuk is de totstandkoming van een privacybeleid doorgenomen. Onderzocht moet worden of het eventuele privacybeleid van het UMCG een goede opbouw heeft en taalkundig makkelijk te begrijpen is voor de betrokkenen. De bepalingen van de EPV, zoals de verplichtingen die verantwoordelijke organisaties hebben en de rechten die de betrokkenen in het privacybeleid terugkomen. Onderzocht moet worden of dit het geval is in het eventuele huidige privacybeleid van het UMCG. Indien deze hier niet aan voldoet, dient geanalyseerd te worden wat er mis is met het privacybeleid en hoe dit verbeterd kan worden.

[102] Grit 2009, p. 14.

6. Implementatie en compliance

6.1 inleiding

Het begrip 'compliance' is al meerdere keren voorgekomen in dit onderzoek. Met deze term wordt aangeduid of de wet- en regelgeving nageleefd wordt. Een organisatie die compliant aan de regelgeving is, leeft de regelgeving naar behoren na. Het kan bij compliance zowel gaan over het naleven van wet- en regelgeving, opgelegd door de overheid, als over het naleven van eigen opgestelde regels binnen de organisatie. Gedacht kan worden aan beleidsregels of gedragscodes. Deze eigen opstelde regels van de organisatie dienen weer aan de nationale wet- en regelgeving te voldoen. [103]

Compliance is een voorwaarde voor verantwoordelijke bedrijfsvoering. Compliance hangt namelijk nauw samen met risicobeheer. Compliance is een manier om de risico's in te perken en te beheersen. Indien een organisatie niet compliant is aan de wet- en regelgeving, brengt dit namelijk risico's met zich mee. Deze risico's zullen vroeg of laat een keer intreden. De gevolgen kunnen erg negatief uitpakken voor de organisatie. Te denken valt aan reputatieschade, bestuurlijke sancties en schadeclaims. Toch zijn er nog veel organisaties die compliance zien als toegevoegde waarde. Om als organisatie compliance perfect beheerst te krijgen, dient er veel tijd en geld geïnvesteerd te worden. Echter blijkt dat gevolgen door het niet-compliant zijn aan de wet- en regelgeving vaak veel meer kost voor organisaties. Alleen al de juridische bijstand die vaak nodig is, kost veel geld. Daarnaast zijn de bestuurlijke sancties voor het niet-compliant zijn aan de privacyregelgeving met de komst van de EPV flink omhoog gegaan. Dit alles zorgt ervoor dat goed compliancemanagement de basis voor het drijven van een verantwoorde organisatie vormt.[104]

6.2 Ziekenhuiscompliance en risicomanagement

Voordat er ingegaan wordt op de compliancecyclus is het belangrijk om te weten wat ziekenhuiscompliance precies inhoudt. Zoals hierboven besproken wordt, valt onder compliance; het bevorderen en handhaven van de naleving van regelgeving. Hieronder valt ook een goed risicomanagement binnen de organisatie. De gevolgen indien de risico's intreden, zoals schade, kunnen door middel van het risicomanagement voorkomen worden. Voor ziekenhuizen wordt dit als volgt omschreven; *'Ziekenhuiscompliance en risicomanagement richt zich op het bundelen en coördineren van het management van bedrijfsrisico's binnen ziekenhuizen met bijzondere aandacht voor het bevorderen en handhaven van de naleving van zowel de externe wet- en regelgeving als de interne reglementen, richtlijnen, procedures en instructies'.*[105]

Ziekenhuiscompliance en een goed risicomanagement kunnen leiden tot verscheidene voordelen. Allereerst krijgt de organisatie meer inzicht in de relevante wet- en regelgeving en in de interne regelgeving. Dit zorgt er gelijk voor dat organisaties zich meer bewust worden van de interne reglementen, richtlijnen, procedures en instructies. In grote organisaties als ziekenhuizen kan de interne regelgeving nogal eens overlappen of kan er onduidelijkheid bestaan over welke regelgeving er precies is binnen de organisatie. Dit kan door het in kaart brengen van alle interne regelgeving zoveel mogelijk voorkomen en/of opgelost worden. Daarnaast hebben organisaties door ziekenhuiscompliance en een goed risicomanagement meer zicht op de naleving van de interne en externe regelgeving. Hierdoor kan het ziekenhuis transparanter te werk gaan jegens betrokkenen en de AP. Uit eerdere theorie is gebleken dat de EPV deze transparantie eist van een organisatie.[106]

[103] Van Leeuwen 2009, p. 95-96.
[104] Van Leeuwen 2009, p. 97-102.
[105] Bleker 2010, p. 6.
[106] Bleker 2010, p. 8.

6.3 De compliancecyclus

De compliancecyclus is een instrument om wet- en regelgeving te implementeren in een organisatie. De compliancecyclus bestaat uit verschillende fasen. Al deze fasen moeten door de organisatie worden doorlopen om de nieuwe wet- en regelgeving in te voeren, met als doel het compliant worden aan de wet- en regelgeving. De compliancecyclus is gericht op continue verbetering. De cyclus stopt dus niet na het afronden van de laatste fase. Indien het ingevoerde niet effectief blijkt te werken of indien de naleving van de regels faalt, moeten er nieuwe maatregelen genomen worden. Er gaat dan weer een nieuwe compliancecyclus van start, waarbij de fasen weer opnieuw doorlopen moeten worden.[107]

Het is van belang dat het bestuur van de organisatie het compliance zijn aan de wet- en regelgeving als belangrijke zaak ziet. Het bestuur van de organisatie is namelijk verantwoordelijk voor de feitelijke naleving van het geïmplementeerde binnen de organisatie. Het is dus van belang dat het bestuur van het UMCG en het hoofd van de afdeling P&O het implementeren van het privacybeleid voor de afdeling P&O als waardevol onderwerp ziet en dit ook laat zien aan de medewerkers. Daarnaast hebben omgevingsfactoren invloed op het succes van het compliancetraject. Een voorbeeld hiervan is de organisatiecultuur, welke voortvloeit uit het gedrag van alle betrokken partijen. Alle partijen dienen individueel het belang van de compliance in te zien. De medewerkers dienen het compliance zijn van de organisatie als eigen verantwoordelijkheid te gaan zien. Zij zullen dit echter niet doen als het bestuur en het management het compliancetraject niet als waardevol beschouwd.[108]

De fasen van de compliancecyclus zijn als volgt;
1. Plannen (Plan)
2. Regels maken en verbeteren (Do)
3. Toezien op naleving (Check)
4. Verbeteren (Act)
In de fasen van de compliancecyclus kunnen de vier stappen van de W. E. Deming herkend worden. Deming was een deskundige op het gebied van kwaliteitscontrole en kwaliteitsmanagement. De cirkel is een verbetercirkel voor kwaliteitsmanagement, gericht op verbetering van ieder willekeurig bedrijfsproces.[109]

6.3.1 Fase 1: Plannen

In de eerste fase dienen alle fasen die doorlopen moeten worden, voorbereid te worden. Er wordt een complianceprogramma gevormd. Over alle stappen van de compliancecyclus moet worden nagedacht en hieruit moet een plan van aanpak voortvloeien. De fasen worden zo gedetailleerd mogelijk omschreven en uitgewerkt in het plan van aanpak, waarna dit moet worden vertaald in activiteiten. Logischerwijs is het van belang om hierbij altijd de betreffende afdeling en organisatie in het achterhoofd te houden. De activiteiten worden als specifiek omschreven; *wie* doet *wat* op *welke wijze* en *manier*. De bedoeling is dat dit op de achtergrond gebeurd, waardoor de medewerkers die bezig zijn met bedrijfsactiviteiten hierin niet of nauwelijks belemmerd worden. Het uiteindelijke complianceprogramma moet zo uitgebreid zijn dat alle verdere stappen op grond hiervan kunnen worden uitgevoerd door de personen die hiervoor gekozen zijn.[110]

<u>De volgende stappen moeten in de eerste fase worden doorlopen;</u>

- ***Inventariseren van de voorschriften***

[107] Van Leeuwen 2009, p. 104-105.
[108] Van Leeuwen 2009, p. 105-106, 122.
[109] Van Leeuwen 2009, p. 104-105.
[110] Van Leeuwen 2009, p. 107.

Allereerst moeten de vereisten die voortvloeien uit de wet- en regelgeving waaraan de organisatie moet voldoen geanalyseerd worden. Bepalingen in de wet- en regelgeving kunnen tamelijk open gelaten zijn. Hierdoor is het voor de organisatie soms niet duidelijk wat er precies van haar wordt verwacht en hoe zij kan zorgen dat de bepalingen nageleefd worden. De bepalingen dienen dan door de organisatie geïnterpreteerd en uitgewerkt te worden in voorschriften die toegespitst zijn op het soort onderneming of afdeling. De interpretatie kan uitgevoerd worden door bepaalde bronnen te raadplegen, zoals toelichtingen bij de regeling, jurisprudentie of de geschiedenis van de wet.[111]

- ***Inventariseren van de ondernemingsactiviteiten die door de regeling worden geraakt***
  De bedrijfsonderdelen, bedrijfsactiviteiten, bedrijfsprocessen of productieprocessen die door de regeling worden geraakt dienen in kaart gebracht te worden in een matrix. Hierdoor ontstaat er een normenkader. Dit zorgt voor een compleet beeld van de regeling en op welke onderdelen deze regeling invloed zal hebben.[112]
- ***Identificeren en analyseren van de risico's van niet-naleving***
  Voor de organisatie moet duidelijk zijn wat er kan gebeuren indien de regeling niet goed nageleefd wordt. Hiervoor dienen de risico's, die ontstaan door het niet-compliance zijn aan de regelgeving, in kaart te worden gebracht. Duidelijk moet worden hoe groot de risico's zijn voor de organisatie, hoe groot de kans is dat de risico's intreden en wanneer en waar dit kan gebeuren. Aanbevolen kan worden om dit vast te leggen in een schriftelijk deel en risicomatrix. Uit de risicomatrix moet blijken aan welke vereisten uit de regelgeving van belang zijn tijdens het analyseren van de risico's en in welke categorieën de risico's kunnen worden opgedeeld.[113] Een voorbeeld van een risicomatrix is weergegeven in bijlage 3 op pagina 80.
- ***Vaststellen van de complianceambitie***
  Vastgesteld moet worden wat de organisatie wil bereiken met de risicobeheersing en wat haar doelstellingen zijn, met daarbij aan welke maatstaven moet worden voldaan.[114]
- ***Bepalen van de maatregelen ter beheersing van het risico van niet-naleving***
  De beheersmaatregelen hebben als doel om naleving van de regeling te bereiken. De verantwoordelijkheden moeten goed verdeeld zijn, bijvoorbeeld door het scheiden van de functies van controlerende en uitvoerende partijen. Hoe gedetailleerd de beheersmaatregelen beschreven dienen te worden hangt af van de grootte en complexiteit van de organisatie. Belangrijk is om ook te kijken welke maatregelen prioriteit hebben, omdat het hele compliancetraject vaak lang duurt.[115]
- ***Vaststellen van tijdpad en deadlines***
  Het tijdpad en de deadlines moeten concreet en duidelijk vastgelegd worden. De implementatie moet voor het verstrijken van de overgangstermijn van de regeling afgerond zijn.

- ***Bepalen welke personen verantwoordelijk zijn voor de uitvoering***
  Vooraf dient bepaald te worden wie verantwoordelijk is voor het uitvoeren van de maatregelen en taken.
- ***Bepalen of er externe deskundigheid of ondersteuning nodig is***
- ***Opstellen van een budget voor het compliancetraject***
- ***Opstellen van het complianceprogramma***

<u>Voor de tweede fase van de cyclus moeten de volgende onderdelen worden uitgewerkt:</u>

[111] Van Leeuwen 2009, p. 108.
[112] Van Leeuwen 2009, p. 108.
[113] Van Leeuwen 2009, p. 109.
[114] Van Leeuwen 2009, p. 110-111.
[115] Van Leeuwen 2009, p. 110-111.

- ***Het vertalen van de regels naar begrijpelijke instructies en procedures***
  In de planning van de tweede fase moeten de voorgeschreven bepalingen van de regeling worden vertaald naar interne regels, zoals beleid, instructies of procedures. De interne regelgeving moet begrijpelijk zijn voor alle partijen die hiermee zullen gaan werken. Dit draagt bij aan het mitigeren van het risico's. Door het lezen van deze interne regelgeving moet duidelijk worden wat de taken zijn, wanneer deze uitgevoerd moeten worden en hoe deze verdeeld zijn. [116]
- ***Het implementeren van de regels in de organisatie***
  Het maken van de interne regelgeving is nu gebeurd. Deze interne regelgeving dient echter ook goed nageleefd te worden, anders is de organisatie nog steeds niet compliant aan de externe regelgeving waaraan zij moet voldoen. In de planningsfase moet erover nagedacht worden hoe bereikt kan worden dat iedereen op wie de interne regels van toepassing zijn, weet welke regels er zijn, wat er van wie verwacht wordt en hoe het verwachte uitgevoerd moet worden. Dit kan door communicatie, training en bewustwording. Het is belangrijk dat communicatie en training duidelijk en tijdig gepland worden. Vastgesteld moet worden hoe de interne regels de verschillende partijen in de organisatie het beste bereiken.
  Dit kan bijvoorbeeld door middel van een presentatie. Ook moet er aan de bewustwording van deze partijen worden gewerkt. Het bewustzijn van de (externe) regelgeving en van de sancties is noodzakelijk voor een goede uitvoering van de interne regelgeving. De partijen moeten gaan beseffen hoe belangrijk naleving van de interne regelgeving is voor de organisatie.

<u>Voor de derde fase van de cyclus moeten de volgende onderdelen worden uitgewerkt:</u>

- ***Bepalen van de vorm, frequentie en intensiteit van het toezicht op naleving***
  Om de vorm, frequentie en intensiteit van het toezicht te bepalen moet er rekening gehouden worden met de omvang van de organisatie, de aard van de regels en de risico's die er zijn als de regels niet goed nageleefd worden.
- ***Prioriteiten bepalen in de monitoringactiviteiten op basis van de risico's***
  Vooraf dient goed gekeken te worden waar aandachtspunten en prioriteiten liggen met betrekking tot de risico's. Er moet een inschatting gemaakt worden van de frequentie en de vormen van het niet-naleven, zodat er op bepaalde aspecten van de naleving specifiek kan worden gelet.
- ***Bepalen op welke wijze, wanneer, door wie en aan wie moeten worden gerapporteerd***
  Ingeschat moet worden hoe vaak en aan wie moet worden gerapporteerd. Belangrijk is om ervoor te zorgen dat de frequentie van het rapporteren haalbaar is voor degene die gaat rapporteren. [117]
- ***Bepalen van de vorm en de inhoud van de rapportages met betrekking tot (niet-)naleving***
  Er moet gekeken worden wat er in de rapportages moet worden gezet en in welke vorm dit gebeurd. Besproken moet worden hoe gedetailleerd de rapportages moeten zijn. Het rapporteren dient schriftelijk te gebeuren, zodat er geen onduidelijkheid over het gerapporteerde ontstaat en de rapportages er te allen tijde bij kunnen worden gepakt.
- ***Bepalen hoe er gehandeld wordt bij geconstateerde niet naleving***
  De organisatie moet bepalen in hoeverre zij wil overgaan tot sanctionering indien er de opgestelde regels niet nageleefd worden. Belangrijk is om dit met het management te bepalen. Er kan ook nagedacht worden of er een beloning volgt indien de regels goed worden nageleefd. [118]

<u>Voor de vierde fase van de compliancecyclus moeten de volgende onderdelen worden uitgewerkt:</u>

[116] Van Leeuwen 2009, p. 112-114.
[117] Van Leeuwen 2009, p. 116-117.
[118] Van Leeuwen 2009, p. 117.

- ***Bepaalt dient te worden wie de beoordeling van de rapportages en de evaluatie van de complianceprestaties op zich neemt***
- ***Er dient criteria opgesteld worden waaraan getoetst wordt welke maatregelen, instructies en procedures verbeterd moeten worden***
- ***Er moet bepaalt worden wanneer de evaluatie en aanbevelingen klaar moeten zijn***
- ***Bepaalt moet worden wie de aandachtspunten bespreekt met de planners***
- ***Er moet iemand aangesteld worden die toezicht houdt of de aanbevelingen en aandachtspunten worden opgevolgd*** [119]

De planning van de fasen twee, drie en vier is nu afgerond. Nu dienen deze fasen nog uitgevoerd te worden. In de volgende paragrafen wordt ingegaan op aandachtspunten en de uitvoering per fase.

6.3.2 Fase 2: Regels maken en verbeteren

De planning van fase twee is in fase 1 uitgewerkt. De (uitvoering van de) tweede fase dient als resultaat te hebben dat het complianceprogramma, dat opgesteld is door middel van het doorlopen van de planning, binnen de tijd wordt afgerond. De activiteiten omtrent het opstellen en implementeren van de interne regels dienen uitgevoerd te worden.
Er zijn enkele aandachtspunten;
- De interne regelgeving moet in begrijpelijke taal geschreven zijn.
- Duidelijk moet zijn op welke bedrijfsonderdelen en processen de regels van toepassing zijn.
- De aanbevelingen, instructies en communicatie moeten duidelijk en concreet zijn.
- Er moet voldoende aandacht worden besteed aan de bewustwording van het belang van het complianceprogramma.[120]

6.3.3 Fase 3: Toezien op naleving

De opgestelde interne regels zijn bij het bereiken van de derde fase geïmplementeerd in de organisatie. In de derde fase dient gecontroleerd te worden of dit ook echt het geval is. De manier van het houden van toezicht en de manier van sanctionering zal per organisatie verschillen. In de planningsfase is al bepaald hoe het toezicht plaats zal vinden. In de derde fase zal de bepaalde manier van toezicht houden uitgevoerd moeten worden. Het resultaat van de derde fase is dan ook; de activiteiten voor controle en toezicht op de naleving van de regelgeving worden binnen de geplande tijd uitgevoerd.
Er zijn enkele aandachtspunten;
- Gekeken moet worden of de manier van toezichthouden ook effectief is.
- Er moet gecontroleerd worden of de frequentie van het controleren wel juist is.
- De taken en verantwoordelijkheden moeten goed en duidelijk verdeeld zijn.
- De uitkomst van de controles worden niet goed of niet tijdig gerapporteerd.[121]

6.3.4 Fase 4: Verbeteren

In de laatste fase van de compliancecyclus wordt gekeken of de doelstelling van de compliancecyclus is behaald. Uit de rapportage van fase drie moet blijken of de organisatie ook echt compliant is aan de (interne) regelgeving. Aan de hand hiervan moet worden bepaald welke maatregelen, regels, instructies en maatregelen verbetering verdienen. De uitkomst hiervan moet worden uitgewerkt in aanbevelingen en maatregelen. Hieruit volgen actiepunten. Het resultaat van de vierde fase moet zijn dat de gegevens en instructies geformuleerd zijn, waardoor de planners een nieuwe cyclusronde kunnen ontwerpen met waarin deze verbetermaatregelen zijn opgenomen.[122]

[119] Van Leeuwen 2009, p. 118-119.
[120] Van Leeuwen 2009, p. 119-120.
[121] Van Leeuwen 2009, p. 120-121.
[122] Van Leeuwen 2009, p. 121.

6.4 Conclusie en onderzoekspunten

Als er nieuwe wet- en regelgeving in opkomst is moet dit geïmplementeerd worden in een organisatie. Een hulpmiddel om dit te bereiken is de compliancecyclus. Deze cyclus bestaat uit vier fases, achtereenvolgens; plannen, regels maken en verbeteren, toezien op naleving en verbeteren. Na de laatste fase begint, indien nodig, een nieuwe cyclus. Als er nieuwe regels verwerkt worden in een privacybeleid moeten de medewerkers binnen de organisatie deze ook naleven, omdat de organisatie anders nog steeds niet compliant aan de EPV is. Dit kan door bewustwording, training en goede communicatie.

Onderzocht moet worden hoe ervoor deze bewustwording gezorgd kan worden bij medewerkers en leidinggevenden, zodat het privacybeleid niet ondergesneeuwd zal worden door werkzaamheden en andere documenten. In het praktijkgedeelte zullen interviews gehouden worden met medewerkers van de afdeling P&O. De onderzoeker is door de interviews in staat om door te vragen naar mogelijke oplossingen voor de problematiek met betrekking tot de werking van het privacybeleid op de werkvloer. De medewerkers worden door een halfgestructureerde interview in staat gesteld om hun mening en zienswijze met betrekking tot compliance en implementatie te delen.

7. Praktijkresultaten

7.1 Resultaten interviews

In dit hoofdstuk worden de praktijkresultaten en bevindingen weergegevens, welke voortvloeien uit de interviews. De interviewvragen worden weergegeven in bijlage 4 op pagina 81 en de uitwerking hiervan in bijlage 5 vanaf pagina 82. De onderzoekspunten die uit de theorie zijn voortgekomen worden zijn deze interviews meegenomen en onderzocht. De geïnterviewde personen worden aangehaald als respondenten. Het hoofdstuk is verdeeld in een aantal paragrafen, waarin de resultaten per onderwerp worden weergegeven. Deze bevindingen en praktijkresultaten geven antwoord op de praktijkgerichte deelvragen.

Ter verduidelijking worden de onderzoekspunten die voortvloeien uit de theorie allereerst per hoofdstuk weergegeven:
Wbp Een onderzoekspunt voortvloeiend uit bovenstaand hoofdstuk is of de regels die de Wbp geeft, momenteel nageleefd worden in het UMCG en in een privacybeleid op zijn genomen. Dit is van belang omdat op dit moment sprake is van een overgangsfase waarin de Wbp nog van toepassing is en de huidige situatie in kaart moet worden gebracht om te kunnen onderzoeken waar verbeterpunten zitten. Op deze manier kan er gekeken worden of de bepalingen van de Wbp goed geïmplementeerd zijn in de organisatie. Indien dit niet het geval is, kan er met de komst van de EPV winst worden behaald bij de implementatie van de nieuwe wet- en regelgeving binnen de afdeling P&O van het UMCG.

EPV Met de komst van de EPV zijn er een talrijk aantal nieuwe verplichtingen voor organisaties. Zo is een FG voor grote organisaties verplicht geworden. Daarnaast moeten de organisaties zorgen voor een privacybeleid, dat ertoe moet leiden dat de organisatie compliant aan de bepalingen van de EPV handelt. Onderzocht moet worden of de afdeling P&O van het UMCG een privacybeleid hanteert. Daarnaast moet onderzocht worden of dit privacybeleid voldoet aan de bepalingen van de EPV. De verplichtingen die de afdeling P&O heeft op grond van de EPV dienen opgenomen te zijn. Daarnaast moeten de rechten die een medewerker als betrokkene heeft in het privacybeleid staan en gefaciliteerd zijn. Tevens moet onderzocht worden of het eventuele privacyreglement aan privacy by design en privacy by default voldoet, of de incidenten met betrekking tot gegevensbescherming aan bod komen en of de organisatie de persoonsgegevens niet langer worden bewaard dan noodzakelijk is.

Totstandkoming privacybeleid Onderzocht moet worden of het eventuele privacybeleid van het UMCG een goede opbouw heeft en taalkundig makkelijk te begrijpen is voor de betrokkenen. De bepalingen van de EPV, zoals de verplichtingen die verantwoordelijke organisaties hebben en de rechten die de betrokkenen in het privacybeleid terugkomen. Onderzocht moet worden of dit het geval is in het eventuele huidige privacybeleid van het UMCG. Indien deze hier niet aan voldoet, dient geanalyseerd te worden wat er mis is met het privacybeleid en hoe dit verbeterd kan worden.

Implementatie en compliance Onderzocht moet worden hoe ervoor deze bewustwording gezorgd kan worden bij medewerkers en leidinggevenden, zodat het privacybeleid niet ondergesneeuwd zal worden door werkzaamheden en andere documenten. In het praktijkgedeelte zijn interviews gehouden met medewerkers van de afdeling P&O. Een onderzoeker kan door middel van interviews als onderzoeksmethode doorvragen naar mogelijke oplossingen voor de problematiek met betrekking tot de werking van het privacybeleid op de werkvloer. De medewerkers worden door het halfgestructureerde interview in staat gesteld om hun mening en zienswijze met betrekking tot compliance en implementatie te delen.

7.1.1 Belangen UMCG

Het UMCG heeft als organisatie meerdere belangen bij een goed werkend privacybeleid. De afdeling P&O beheert als afdeling het personeelsadministratiesysteem. Hierin wordt alle data ruim 12.000 medewerkers opgeslagen. Op het moment dat een medewerker uitvindt dat zijn of haar personeelsgegevens niet goed beveiligd zijn of zonder goede redenen gedeeld wordt met anderen, zal zij ontevreden worden. Dit zorgt ervoor dat de medewerker een stuk vertrouwen verliest in het UMCG als werkgever en daardoor minder snel persoonlijke problemen of gegevens zullen durven te delen. Hierdoor zal het UMCG niet vooruitstrevend en anticiperend te werk kunnen gaan met betrekking tot haar personeel. Een voorbeeld van een consequentie hiervan is dat een medewerker niet het vertrouwen heeft om een burn-out tijdig te melden aan het UMCG. Het UMCG kan dan niet vroegtijdig maatregelen treffen om ervoor te zorgen dat de burn-out niet gaat leiden tot langdurig ziekteverzuim. Tevens heeft het UMCG belang bij een goed privacybeleid omdat zij als organisatie een bestuurlijke boete opgelegd kan krijgen van de hoogste categorie indien zij geen privacybeleid hanteert. Daarnaast heeft het UMCG er belang bij als zij niet negatief in de publiciteit terecht komt omdat zij als organisatie de gegevensverwerking niet op orde heeft, gegevens op straat komen te liggen of een bestuurlijke boete opgelegd krijgt. Hierdoor zullen verschillende partijen niet meer met het UMCG in zee durven gaan. De andere kant hiervan is het bieden van kwaliteit. Indien het UMCG als organisatie de gegevens compliant aan de EPV verwerkt in een intern privacybeleid, welke voor medewerkers duidelijk en uitvoerbaar is, zullen medewerkers hun gegevens hoogstwaarschijnlijk eenvoudiger durven delen. De afdeling P&O weet zo meer van de medewerkers, waardoor zij krachtdadig en voortvarend te werk kan gaan. Derde partijen zullen meer vertrouwen op de professionaliteit van het UMCG als bedrijf, indien zij EPV compliant te werk gaat. Bovenstaande heeft als gevolg dat het UMCG als organisatie veel belang heeft bij een goed werkend privacybeleid.

7.1.2 Belangen medewerkers

Naast de belangen die het UMCG als organisatie heeft, hebben de medewerkers ook verschillende belangen bij een goed werkend privacybeleid. Allereerst omdat bij de gegevensverwerking van de afdeling P&O de medewerkers de betrokkenen zijn, waarvan de gegevens verwerkt worden. Er worden namelijk bij de afdeling P&O gegevens verwerkt omtrent personele data. De personele data die verwerkt wordt is persoonlijk en daarmee voor een groot deel vertrouwelijk. Als medewerker is het uiterst vervelend als collega's en andere partijen vertrouwelijke gegevens onder ogen krijgen. Het delen van deze gegevens kan ertoe leiden dat een medewerker bij een andere werkgever niet aangenomen wordt, omdat er bijvoorbeeld sprake was van ziekteverzuim of te laat komen. De medewerkers die de persoonsgegevens juist verwerken hebben een ander belang. Zij hebben er namelijk belang bij dat zij weten hoe zij dit moeten doen, zodat er geen fouten gemaakt worden. Fouten kunnen, naast een vervelende werksfeer, grote consequenties tot gevolg hebben. Het privacybeleid moet voor deze partij laagdrempelig en geconcretiseerd zijn. Hierdoor kunnen zij hun werkzaamheden goed uitvoeren.

7.1.3 Werking privacybeleid

Om de gegevens uit de theorie met de praktijk te kunnen vergelijken, moet in kaart gebracht worden wat er op dit moment is aan privacybeleid op de afdeling P&O. Het UMCG is toe aan een gestructureerd privacybeleid. Tot op heden heeft een privacybeleid geen prioriteit gehad. De komst van de EPV heeft dit veranderd. In de volgende subparagrafen is beschreven hoe dit volgens de geïnterviewde personen in elkaar steekt op de afdeling P&O.

Schriftelijk beleid

Op dit moment is er sprake van een privacyreglement bij de afdeling P&O. Dit privacyreglement is UMCG breed en stamt uit 2005. Echter wordt er van dit beleid geen gebruik gemaakt op de werkvloer. De 4 van de 7 respondenten weten niets af van het privacyreglement. Het privacyreglement is weergegeven in bijlage 6 op pagina 94.

Het personeelsadministratiesysteem is opgedeeld in verschillende bevoegdheden per functie. Per functie is namelijk bepaald in hoeverre een medewerker bij bepaalde personeelsdata behoort te kunnen. Sommige medewerkers kunnen de personeelsgegevens niet inzien, sommige medewerkers kunnen de personeelsdata maar voor een klein deel inzien en enkele medewerkers kunnen alle personeelsdossiers volledig inzien. Daarnaast kunnen alleen bepaalde medewerkers de gegevens muteren. De medewerkers krijgen een rol afhankelijk van de functie. Ieder jaar wordt er controle uitgevoerd of alle bevoegdheden correct zijn ingevoerd. Medewerkers zijn op de hoogte van het doel van de gegevensverwerking indien zij de arbeidsovereenkomst tekenen. Hierin wordt namelijk een basis set aan data gevraagd. Van de medewerkers wordt verwacht dat zij zich dan beseffen dat deze gegevens verwerkt zullen worden. De respondenten die een functie hebben als medewerker zeggen dat zij zich dat wel beseffen, maar dat er nimmer expliciet op gegevensverwerking gewezen wordt.

Er is ook een UMCG-brede gedragscode welke beschrijft hoe medewerkers zich over het algemeen dienen te gedragen op de werkvloer. Deze gedragscode is te vinden in bijlage 7 vanaf pagina 101. Daarnaast is er een UMCG-brede gedragscode waarin beschreven wordt hoe medewerkers zich dienen te gedragen met betrekking tot internetgebruik. Deze gedragscode is te vinden in bijlage 8 vanaf pagina 108. Bij het opstellen van deze gedragscodes is rekening gehouden met privacy. Drie respondenten geven aan deze gedragscode te kennen.

Ongeschreven beleid

Van iedere medewerker wordt verwacht dat deze zich als een goed medewerker gedraagt. Indien er zich bijzondere situaties voordoen op de afdeling P&O omtrent de verwerking van gegevens, wordt er van de medewerkers verwacht dat deze overleg voert met de leidinggevenden over de wijze waarop dit moet gebeuren. Bijzondere situaties zijn situaties van gegevensverwerking die niet omschreven zijn in het privacyreglement.

Op de afdeling P&O wordt er volgens drie respondenten enigszins gediscussieerd onder welke omstandigheden gegevens wel of niet verwerkt mogen worden. Tijdens deze discussies wordt volgens deze respondenten rekening gehouden met de wet- en regelgeving en daarmee met de bepalingen van de EPV. Wat er besproken en afgesproken wordt, wordt echter niet schriftelijk vastgelegd.

Door de samenwerking met de opleiding Geneeskunde worden er gegevens uitgewisseld met de Rijksuniversiteit Groningen van bijvoorbeeld stagiaires. Deze gegevensoverdracht moet voldoen aan de bepalingen van de EPV. Er wordt in vergaderingen overlegd welke data moet en mag worden uitgewisseld. Hieraan wordt veel aandacht besteedt door de afdeling P&O.

Er zijn veel gegevens die verwerkt worden terwijl de medewerker hier niet expliciet op wordt gewezen. Dit zijn veelal gegevens die verplicht moeten worden vastgelegd op grond van wettelijke verplichtingen zoals de sociale verzekeringswetgeving. Daarnaast worden de papieren met vertrouwelijke gegevens gedeponeerd in speciale vuilnisbakken of deze papieren gaan in de papierversnipperaar. Alle respondenten geven aan dat dit erg goed nageleefd wordt op de afdeling en dat ieder hiervan het belang inziet.

Bij ziekteverzuim wordt er gebeld met leidinggevenden of met de secretaresse van de leidinggevenden. De gegevens omtrent het ziekteverzuim worden opgeslagen en opgenomen in het personeelsdossier. Op de afdeling zijn de leidinggevenden en secretaresses bewust bezig met de ziekteverzuimregistratie. Het Arbo-systeem is afgesloten van de andere gegevens. De leidinggevenden en secretaresses kunnen het ziekteverzuim invoeren. Het weder inzien van de ziekteverzuimregistratie kan alleen de leidinggevende.

7.1.4 Aandachtspunten omtrent privacybeleid

Medewerkers met leidinggevende functies op de afdeling P&O hebben meegekregen dat er nieuwe

privacywetgeving in opkomst is. De komst van de EPV brengt een aantal aandachtspunten en problemen mee voor het UMCG als er naar de resultaten uit de interviews gekeken wordt.

Allereerst is het van belang om op te merken dat er wel sprake is van een privacyreglement, maar dat dit pas in de laatste interviews naar voren is gekomen. Menig leidinggevende en medewerker is niet goed op de hoogte van het privacyreglement. Het privacyreglement staat gepubliceerd op intranet van het UMCG, maar wordt zodanig ondergesneeuwd door andere documenten dat er in de organisatie (bijna) geen weet van het bestaan van het reglement is. Een secretariële respondent geeft aan te weten van het privacyreglement, omdat deze tijdens haar werkzaamheden het intranet goed moet volgen. Deze respondent werd als vijfde geïnterviewd, maar was de eerste respondent die op de hoogte was van het privacyreglement. Naast deze respondent waren er nog twee respondenten die wisten van het privacyreglement. Omdat er van het overgrote deel van de respondenten geen weet is van het reglement, hebben de respondenten geen idee wat hun rechten zijn en wat de verplichtingen, die de organisatie als gegevensverwerker heeft, zijn. Tevens kan hieruit geconcludeerd worden dat de implementatie van het privacyreglement niet geslaagd is, omdat het reglement nauwelijks bekend is op de werkvloer.

Daarnaast stamt het privacyreglement oorspronkelijk uit 2003 en is deze aangepast in 2005. Het zal dus ongetwijfeld erg verouderd zijn.

Ook worden de medewerkers niet gewezen op het doel van de gegevensverwerking. De afdeling P&O dient te allen tijde de medewerker in begrijpelijke vorm en taal alle informatie met betrekking tot de verwerking van zijn of haar persoonsgegevens te verschaffen. Op dit moment gebeurd dit volgens verschillende respondenten nog niet. Veelal lijkt er te snel aangenomen te worden dat de medewerkers wel weten dat hun persoonsgegevens verwerkt worden. In bepaalde omstandigheden, bijvoorbeeld bij de aanstelling, worden zelf gegevens ingevoerd door de medewerker. Hier wordt aangenomen dat deze medewerker ook op de hoogte is dat de gegevens daarna verwerkt zullen worden.

Momenteel worden de medewerkers niet expliciet gewezen op de rechten die zij hebben indien hun persoonsgegevens als personele data worden verwerkt. De betrokkenen worden bijvoorbeeld niet gewezen op het recht tot rectificatie of het recht op het wissen van zijn of haar persoonsgegevens. Ook worden zij niet expliciet gewezen op het recht om bezwaar te maken tegen de verwerking van persoonsgegevens betreffende de betrokkene. Wel wordt er zo nu en dan inzage gevorderd door een medewerker in zijn of haar personeelsdossier. Het lijkt erop dat de betrokkenen dus wel van het recht op inzage op de hoogte zijn.

Daarnaast is een aandachtspunt dat twee respondenten aangeven dat veel medewerkers hun werkmail koppelen aan hun privételefoon. De afscherming hiervan is gering. Alleen de toegangscode van de telefoon is vaak voldoende om in de werkmail te komen. Indien een telefoon bijvoorbeeld gestolen wordt en gekraakt wordt, kan een willekeurig persoon met één klik op de werkmail binnenkomen. In deze werkmail staat veelal vertrouwelijke informatie. Binnen de afdeling P&O van het UMCG is hier niets over geregeld.

Tevens is er nog het aandachtspunt dat de kamers en kasten waar een slot op zit, te allen tijde gesloten dienen te worden. Er wordt van de medewerkers verwacht dat zij dit weten en ook doen. De medewerkers zijn hiervan op de hoogte en wijzen elkaar hierop. Alle documenten met persoonsgegevens liggen in dat geval onbeheerd op de kamers. Ook geeft één respondent aan dat de sloten van de kasten wel eens kapot zijn, maar dat het dan weken kan duren voordat deze gemaakt worden. Dit heeft misschien meer betrekking op een gedragscode dan op het privacyreglement, maar één respondent had hierdoor het idee dat het sluiten van de kasten en daarmee een stuk privacy niet als zodanig waardevol en belangrijk wordt gezien door het UMCG zelf.

De komst van de EPV is nog erg vaag op de werkvloer. De leidinggevenden en hoofden van de afdeling P&O hebben al gehoord over de nieuwe regelgeving, maar op de werkvloer wordt hier nog niet echt met medewerkers over gecommuniceerd. Twee respondenten geven aan dat er met brieven en folders is gecommuniceerd over bestuurlijke boetes en datalekken. Hierin wordt echter niet gedefinieerd wanneer er sprake is van een datalek en hoe er in zo'n geval gehandeld dient te worden. Alles is op dit moment nog onduidelijk onder de medewerkers. De komst van de EPV lijkt ondergesneeuwd te worden door andere regels die in de organisatie gelden en medewerkers zien de noodzaak er (nog) niet van in om zich in de EPV-kwestie te gaan verdiepen. Hoe eerder aan het bovenstaande aandacht wordt besteed, hoe eerder de medewerkers kunnen gaan nadenken over het belang van privacy voor een organisatie als het UMCG. Daarnaast wordt er bij de komst van de EPV gelijk gedacht aan het verwerken van patiëntgegevens. Twee respondenten geven aan dat ze alleen wisten dat het verwerken van patiëntgegevens strikter zou worden.

De documenten die personeelsgegevens bevatten dienen naar het archief te gaan om vertrouwelijk opgeslagen te worden. Dit gaat via het secretariaat. De documenten dienen hier afgeleverd te worden en worden daarna naar het archief gebracht. Er is een respondent die heeft gevraagd of het opsturen van de documenten in een envelop toegestaan is. Deze kreeg te horen dat dit niet mag met het oog op privacy. De documenten die toen afgeleverd werden bij het archief, moesten daar vervolgens op een onbemand bureau neergelegd worden. Hier stelt een enkele respondent zichzelf de vraag; *hoe belangrijk is privacy dan voor de organisatie?*

Voorheen diende er op de computer twee wachtwoorden ingevuld te worden om in de personeelsdossiers terecht te komen; het wachtwoord van de computer en het wachtwoord van het personeelssysteem. Op dit moment is dit niet meer het geval. Indien een medewerker, die recht heeft om in te loggen op het personeelssysteem, inlogt op zijn of haar computer, kan het personeelssysteem zo aangeklikt worden. Je bent als medewerker dan automatisch ingelogd. Omdat de computers wel eens onbemand achtergelaten worden is dit zorgelijk.

Daarnaast is een aandachtspunt dat het steeds vaker voorkomt dat werknemers ook thuis werken. Indien medewerkers thuis werken lijken deze regels van ongeschreven beleid enigszins te vervallen. Medewerkers geven aan dat er geen regels zijn omtrent het thuiswerken. Er wordt toegegeven dat de documenten thuis meer dan eens onbemand zijn.

7.1.5 Compliance en implementatie EPV

Door drie van de zeven respondenten wordt aangegeven dat de komst van de EPV een ondergesneeuwd onderwerp is binnen de afdeling P&O. Er wordt drie respondenten met leidinggevende functies aangegeven dat zij zich wel tot op een zekere hoogte bezighouden met de EPV. Door vier respondenten geven aan dat de aandacht op de werkvloer niet uitgaat naar de EPV. Als er al aandacht aan de EPV wordt besteed, is dat vaak niet gericht op het privacybeleid, maar meer op patiëntgegevens. Alle respondenten zien als individu wel in dat privacy heel belangrijk is binnen het UMCG en proberen elk op eigen wijze te zorgen dat de privacy gewaarborgd wordt. Ieder individu probeert zelf in te vullen deze het beste met privacygevoelige informatie om kan gaan, omdat het geldende privacyreglement nauwelijks bekend is op de werkvloer.

Er wordt al wel nagedacht over hoe bewustwording met betrekking tot de komst van de EPV en daarmee een verplicht privacybeleid het beste bereikt kan worden. Binnenkort participeren de decentrale personeelsfunctionarissen in een workshop van de Project EPV. Er wordt tijdens deze workshop een spel gespeeld. In dit spel komen de aspecten van de privacyverordening per specifieke werkzaamheid naar voren. Deze workshop moet nog gepland worden.

Het bewustzijn met betrekking tot de komst van de EPV is onder de medewerkers nog niet zo groot als het zou moeten zijn. De medewerkers staan er wel voor open om te leren hoe zij goed met het

privacybeleid om moeten gaan en wat de regels zijn, maar geven duidelijk aan dat zij niet willen dat er een groot document met moeilijke regels zonder uitleg verstrekt wordt.

7.2 Praktijkresultaat privacyreglement

Uit de interviews is gebleken dat er sprake is van een privacyreglement. Omdat dit een belangrijk praktijkresultaat is, wordt dit privacyreglement apart besproken in deze paragraaf. Een onderzoekspunt dat voortvloeide uit de theorie is dat een eventueel privacybeleid dat geldend is op de afdeling P&O compliant moet zijn aan de bepalingen van de EPV. De bepalingen van het privacyreglement zullen in deze paragraaf per artikel besproken worden. In het volgende hoofdstuk wordt geanalyseerd of het privacyreglement aan de bepalingen van de EPV voldoet, omdat de EPV onder het theoriegedeelte valt.

Achtergrond en begripsbepalingen

Op de afdeling P&O is op dit moment in de praktijk een reglement geldend betreffende de bescherming van persoonsgegevens van medewerkers van het UMCG. Dit privacyreglement is opgesteld en in werking gegaan in het jaar 2005. Dit reglement is vastgesteld na instemming van de Ondernemingsraad (OR). Wijzigingen in het reglement kunnen slechts worden doorgevoerd met instemming van de OR. Het reglement is ingegaan op 1 februari 2003 en is gewijzigd in september 2005. In dit hoofdstuk wordt in subparagrafen uiteengezet welke bepalingen volgens de theorie aanwezig behoren te zijn en welke bepalingen er op dit moment in het privacyreglement van de afdeling P&O verwerkt zijn.

In het privacyreglement wordt beschreven dat de Wbp de bepalingen geeft waaraan voldaan moet worden door de organisatie. Ook wordt de Wet op de Ondernemingsraden (WOR) en de Archiefwet aangehaald. Volgens de WOR heeft de OR een instemmingsrecht over een privacyregeling. De Archiefwet bevat bepalingen met betrekking tot bewaartermijnen van persoonsgegevens met oog op de arbeidsovereenkomst. De Raad van Bestuur geeft in het reglement aan dat deze het zorgvuldig omgaan met persoonsgegevens van medewerkers als een belangrijk punt ziet. Omdat er per doeleinde verschillende regels met betrekking tot het verwerken van persoonsgegevens zijn, wordt er in het reglement ruimte gelaten zodat er nadere (uitvoerings)regels gesteld kunnen worden. In de begripsbepalingen wordt als verantwoordelijke de Raad van Bestuur aangemerkt. De definitie van een persoonsgegeven, bewerker, verwerking van persoonsgegevens, toestemming en bestand zijn letterlijk overgenomen uit de Wbp. Ook wordt gedefinieerd wat een Functionaris voor de Gegevensbescherming is. Volgens het privacyreglement is de betrokkene de medewerker waarvan de gegevens verwerkt worden. Wat een medewerker is in de zin van het reglement is omvangrijk uitgeschreven. Waarschijnlijk is dit gedaan omdat het UMCG met veel verschillende soorten medewerkers te maken heeft. Onder medewerkers wordt samenvattend verstaan; een medewerker die aangesteld is bij het UMCG op grond van de CAO Academische Ziekenhuizen. Indien een medewerker niet op grond van deze CAO is aangesteld, maar feitelijk wel bij het UMCG werkt, is deze ook medewerker in de zin van het privacyreglement. Gedacht kan worden aan een persoon met een aanstelling bij de Rijksuniversiteit Groningen, een detacheringovereenkomst, een uitzendkracht en een persoon met een opdracht namens de Raad van Bestuur. Ook vallen stagiaires, studenten en vrijwilligers onder medewerkers. Een persoon dat niet meer valt onder deze begrippen, maar waarvan nog wel persoonsgegevens opgeslagen zijn, valt in de zin van het reglement ook onder medewerker.

Reikwijdte van het reglement

Het reglement dat geldend is in de praktijk, is van toepassing op alle verwerking van persoonsgegevens betreffende medewerkers binnen het UMCG. Zoals hierboven beschreven worden de persoonsgegevens per doeleinde ingedeeld. De volgende doeleinden van gegevensverwerking worden afzonderlijk genoemd; personeels- en salarisadministratie, verwerkingen betreffende

werkarchieven, personeelsarchief, arbo-zorgsysteem, een toegangscontrole- en volgsysteem en een systeem betreffende de uitgifte en inname van bedrijfskleding. Het reglement is ook van toepassing op toekomstige soorten verwerkingen. Hiervoor mogen nadere regels gesteld worden binnen de lijnen van het reglement.

Doelstellingen voor gegevensverwerking
In het reglement dat geldend is in de praktijk zijn algemene doelstellingen opgenomen. De persoonsgegevens van medewerkers mogen alleen worden verwerkt indien de organisatie één van deze doelstellingen voor ogen heeft. Deze doelstelling worden opgesteld door de Raad van Bestuur met instemming van de ondernemingsraad. De doelstellingen zijn als volgt; het geven van leiding aan de werkzaamheden, de behandeling van personeelszaken, het vaststellen en uitbetalen van salaris, het regelen van uitkeringen, de opleiding of ontwikkeling van de betrokkene, de bedrijfszorg van betrokkene, het bedrijfsmaatschappelijk werk, ziektebegeleiding en casemanagement, de verkiezing van de leden van het medezeggenschapsorgaan, de interne controle en beveiliging, de uitvoering van arbeidsvoorwaarden, het verlenen van ontslag, de administratie van personeelsvereniging, het innen van vorderingen, het behandelen van geschillen en de (tijdelijke) overgang van de betrokkene naar een andere afdeling of andere organisatie.

Onverminderd deze doelstellingen mogen persoonsgegevens van medewerkers alleen verwerkt worden indien aan de volgende voorwaarden is voldaan; als een medewerker zijn ondubbelzinnige toestemming heeft gegeven voor de verwerking, als er een wettelijke plicht is op grond waarvan het UMCG de gegevens dient te verwerken, als dit noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het bestuursorgaan waaraan de gegevens worden verstrekt of indien het gerechtvaardigde belang van het UMCG prevaleert boven het recht op bescherming van de persoonlijke levenssfeer van de betrokkene.

De Raad van Bestuur is er daarnaast verantwoordelijk voor dat bij elke verwerking bepaalde normen in acht moeten worden genomen. Deze normen zijn; dat de verwerking van de persoonsgegevens alleen is toegestaan als dit verenigbaar is met de doeleinden waarvoor de persoonsgegevens zijn verkregen, dat er maatregelen getroffen worden die ervoor zorgen dat de persoonsgegevens juist en nauwkeurig zijn, dat de persoonsgegevens zoveel mogelijk bij de betrokkene verkregen worden en dat er zodanige technische en organisatorische maatregelen getroffen worden. Hierdoor dient er sprake te zijn van een adequate beveiliging tegen verlies en onrechtmatige verkrijging van persoonsgegevens. Daarnaast stelt de Raad van Bestuur een FG aan. Door de directie van de afdeling P&O wordt een privacy officer medewerkersgegevens aangesteld.

Bijzondere persoonsgegevens mogen binnen het UMCG alleen verwerkt worden als de Wbp dit toestaat, de betrokkene ondubbelzinnig toestemming heeft gegeven voor de verwerking, de persoonsgevens door de betrokkene zelf duidelijk openbaar zijn gemaakt, de verwerking noodzakelijk is voor een recht in rechte of volkenrechtelijke verplichting.

Bewaartermijnen
Volgens het reglement dat geldend is in de praktijk mogen persoonsgegevens van een medewerkers die uit dienst zijn, tot twee jaar na uitdiensttreding bewaard blijven. Na deze twee jaren moeten de gegevens zo spoedig als redelijkerwijs mogelijk is verwijderd worden. Dit hoeft niet indien; de persoonsgegevens noodzakelijk bewaard moeten worden op grond van een wettelijke plicht, de persoonsgegevens zo bewerkt zijn dat herleiding naar de betrokkene redelijkerwijs onmogelijk is of het UMCG een gerechtvaardigd belang heeft voor het langer bewaren van de persoonsgegevens en de betrokkene hier schriftelijk van op de hoogte is gesteld. De bewaartermijn geldt niet indien deze voor historische, statistische of wetenschappelijke doeleinden worden bewaard, en het UMCG de nodige voorzieningen heeft getroffen om te verzekeren dat deze gegevens uitsluitend voor deze specifieke doeleinden worden gebruikt.

Verplichtingen organisatie
De informatieplicht is de eerste verplichting van het UMCG die is opgenomen in het reglement dat geldend is in de praktijk. Verder staat er onder de informatieplicht dat gemeld moet worden bij de privacy officer indien er gegevens verwerkt worden op grond van andere doelstellingen dan genoemd in reglement. De documentatieplicht in het Register van de verwerkingsactiviteiten is opgenomen in het privacyreglement. Er staat namelijk dat de Raad van Bestuur een document dient bij te houden met het specifieke doel van de verwerking, een beschrijving van de opzet van de verwerking, de categorieën medewerkers, aan welke personen of instanties de persoonsgegevens verstrekt zouden kunnen worden, de beveiligingsmaatregelen en de rollen van de FG en de security privacy officer met betrekking tot de persoonsgegevensverwerking. De Raad van Bestuur moet daarnaast op grond van het reglement passende technische en organisatorische maatregelen treffen om de persoonsgegevens te beveiligen.

Rechten betrokkenen
In het reglement dat geldend is in de praktijk staan enkele rechten van betrokkenen vermeld. Allereerst is het recht op inzage vermeld. Het verzoek tot inzage moet binnen vier weken afgehandeld zijn. Het verzoek kan worden geweigerd ter bescherming van de rechten of verplichtingen van anderen. Deze weigering moet volgens het reglement schriftelijk met redenen geschieden. Daarnaast heeft elke medewerker het recht op correctie of op afscherming van de persoonsgegevens. Dit recht heeft de medewerker indien de gegevens onjuist zijn, voor het doel niet dienend zijn of in strijd zijn met een (wettelijk) voorschrift of een regeling. De privacy officer neemt binnen vier weken beslissing op het verzoek tot wijziging en/of afscherming. Een weigering wordt schriftelijk met redenen gegeven. Als een medewerker het niet eens is met de beslissing op het verzoek tot inzage, wijziging, verbetering of aanvulling, dan kan deze een bezwaarschrift indienen bij de Raad van Bestuur. Binnen zes weken wordt hierop beslist. Indien de medewerker het hier niet mee eens is kan deze naar de bestuursrechter gaan. Ook kan de medewerker zich melden bij het CBP. Het recht van bezwaar staat vermeld in het artikel over rechtsbescherming.

Rechtsbescherming
Uit het reglement blijkt dat als een medewerker het niet eens is met een beslissing op een verzoek tot inzage, een beslissing tot afwijzing van het verzoek tot correctie, afscherming, verbetering of aanvulling van persoonsgegevens of een beslissing naar aanleiding van een aantekening van verzet kan deze een bezwaarschrift indienen bij de Raad van Bestuur.

Taalgebruik, toegankelijkheid en formulering
Het reglement dat geldend is afgestemd op de medewerker geschreven. Duidelijk te zien is dat de rechten van de betrokkenen, welke erg van belang zijn voor de medewerker, in begrijpelijke niet-juridische taal is geschreven. Verder staan er in het privacyreglement wel enkele juridische termen die voor de leek misschien niet eenvoudig zijn, zoals bijvoorbeeld volkenrechtelijke verplichting en publiekrechtelijke taak.

7.3 Conclusie
De onderzoekspunten die voort zijn gekomen uit het theoriegedeelte dienen in het praktijkgedeelte onderzocht te worden. Allereerst is onderzocht of de bepalingen uit de Wbp goed geïmplementeerd zijn op de werkvloer. Dit was niet het geval. Daarnaast is onderzocht of er sprake is van een privacybeleid. Er blijkt sprake te zijn van een privacyreglement. Of het privacyreglement aan de bepalingen van de EPV voldoet wordt in het volgende hoofdstuk besproken, omdat de bepalingen van de EPV onder het theoriegedeelte vallen. In het volgende hoofdstuk zal de theorie met de praktijk vergeleken worden. Bovendien is er in de interviews in gegaan op hoe het toekomstige privacybeleid het beste geïmplementeerd kan worden op de werkvloer. Geconcludeerd kan worden dat alle onderzoekspunten uit de theorie zijn gekomen in de praktijk en onderzocht zijn.

8. Analyse

8.1 Inleiding

In dit hoofdstuk worden analyses uiteengezet die voortvloeien uit het vergelijken van het theoretische literatuuronderzoek met onderzoekspunten en het praktijkonderzoek. In dit hoofdstuk wordt de volgende deelvraag onderzocht:

- *Wat kan er worden geconcludeerd als de theorie en praktijk met elkaar vergeleken worden?*

8.2 Analyse compliance en implementatie EPV

Uit de theorie blijkt dat een organisatie dient te voldoen aan bepaalde wet- en regelgeving, gebruik kan maken van de compliancecyclus. De compliancecyclus is een instrument om wet- en regelgeving te implementeren in een organisatie. De compliancecyclus bestaat uit verschillende fasen en is gericht op continue verbetering. Om het compliancetraject succesvol af te ronden, dienen het bestuur en de medewerkers met leidinggevende functie het belang van een goede implementatie in te zien. Zij hebben namelijk een voorbeeldfunctie. Daarnaast hebben omgevingsfactoren, zoals de cultuur binnen de organisatie, invloed op het slagen van het compliancetraject.

Uit de praktijkresultaten blijkt dat (de afdeling P&O van) het UMCG nog niet compliant is aan de bepalingen van de EPV. Er is wel een privacyreglement, welke is afgestemd op de bepalingen van de Wbp. De respondenten geven aan dat dit privacyreglement weinig bekendheid kent op de werkvloer en er ondergesneeuwd wordt door andere documenten en werkzaamheden. Over de EPV wordt volgens de respondenten eigenlijk niet gecommuniceerd. De respondenten geven aan dat zij graag willen dat het privacybeleid eenvoudig te lezen en toegankelijk is. Zij zien er erg tegenop om een heel boekwerk door te gaan lezen, dus beknoptheid zal op de werkvloer gewaardeerd worden. De respondenten willen graag dat de veranderingen specifiek per werkzaamheid worden doorgegeven, zodat zij zelf niet moeten uitzoeken wat er precies anders moet. De respondenten geven aan dat zij het belang van een EPV-compliant en een goed werkend privacybeleid inzien.

De analyse die uit bovenstaande tekst voortvloeit, is dat de medewerkers erg tegen de nieuwe wet- en regelgeving op zien. Ze zien echter het belang van een goed werkend privacybeleid op de afdeling wel in en staan open voor de veranderingen binnen de organisatie. De implementatie van huidig privacyreglement kan niet geslaagd genoemd worden als de theorie met de praktijk vergeleken wordt, aangezien maar drie respondenten weet hebben van het privacyreglement. Het implementeren van het nieuwe privacybeleid verdient dus extra aandacht.

8.3 Analyse privacyreglement

De bepalingen uit het privacyreglement zullen hier samengevat besproken worden om overbodige herhaling te voorkomen. In het hoofdstuk met praktijkresultaten zijn deze bepalingen namelijk helemaal uitgelicht.

8.3.1 Achtergrond en begripsbepalingen

Uit de theorie blijkt dat het de EPV de bepalingen geeft waaraan het privacybeleid moet voldoen. Dit dient dan ook terug te komen in de achtergrond en begripsbepalingen van een privacybeleid. Volgens de theorie zijn de volgende begrippen van belang voor de afdeling P&O van het UMCG: Persoonsgegevens, bijzondere persoonsgegevens, verwerking, beperken van de verwerking, pseudonimisering, verwerker, verwerkingsverantwoordelijke, betrokkene, toestemming, inbreuk in verband met persoonsgegevens en gegevens over gezondheid. Toestemming van de betrokkene is geen gegarandeerde voorwaarde voor het verwerken van persoonsgegevens van medewerkers.

In het reglement dat geldend is in de praktijk staat dat de Wbp de bepalingen geeft waaraan voldaan moet worden door de organisatie. Ook worden de Wet op de Ondernemingsraden (WOR) en

de Archiefwet aangehaald. Omdat er per doeleinde verschillende regels met betrekking tot het verwerken van persoonsgegevens zijn, wordt er in het reglement ruimte gelaten zodat er nadere (uitvoerings)regels gesteld kunnen worden. De verantwoordelijke in de zin van het reglement is de Raad van Bestuur. De definitie van een persoonsgegeven, bewerker, verwerking van persoonsgegevens, toestemming en bestand zijn overgenomen uit de Wbp. Ook wordt Functionaris voor de Gegevensbescherming uitgelegd. Volgens het privacyreglement is de betrokkene de medewerker waarvan de gegevens verwerkt worden. Wat een medewerker is in de zin van het reglement is omvangrijk uitgeschreven.

De analyse die uit bovenstaande tekst voortvloeit, is dat in het reglement dat werkzaam is in de praktijk afgestemd is op de bepalingen van de Wbp. Het reglement moet volgens de theorie afgestemd worden op de bepalingen van de EPV. Er ontbreken enkele begrippen in het huidige reglement volgens de theorie die wel van belang kunnen zijn in het privacybeleid van het UMCG, namelijk: bijzondere persoonsgegevens, beperken van de verwerking, pseudonimisering, inbreuk in verband met persoonsgegevens en gegevens over gezondheid. Daarnaast is het begrip de 'verantwoordelijke' vervangen door de 'verwerkingsverantwoordelijke' en het begrip de 'bewerker' vervangen door de 'verwerker'. Enkele begrippen zijn in definitie veranderd, namelijk; persoonsgegevens, betrokkene, verwerking, bijzondere persoonsgegevens en verwerker. Het begrip toestemming van betrokkene kan mijns inziens het beste verwijderd worden uit de begripsbepalingen, omdat toestemming van betrokkene geen gegarandeerde voorwaarde meer is voor een rechtmatige verwerking van persoonsgegevens. De begrippen die in deze alinea niet behandeld worden, staan gezien de theorie goed in het reglement.

8.3.2 Reikwijdte van het reglement

Uit de theorie blijkt dat de reikwijdte van de EPV ten eerste bepaald wordt door de begrippen 'persoonsgegevens' en 'verwerken'. De EPV is namelijk alleen geldend als er sprake is van een persoonsgegeven en dit persoonsgegeven verwerkt wordt. Dit is het geval bij de persoonsgegevensverwerkingen die in het reglement staan. De verordening is ook van toepassing op verwerkingen van persoonsgegevens, die in een bestand zijn opgenomen of worden opgenomen. Deze EPV is territoriaal van toepassing op de verwerking van persoonsgegevens door een verantwoordelijke of een verwerker in de Europese Unie.

Het reglement dat geldend is in de praktijk, is van toepassing op alle verwerking van persoonsgegevens betreffende medewerkers binnen het UMCG. Zoals hierboven beschreven, worden de persoonsgegevens per doeleinde ingedeeld. Het reglement is ook van toepassing op toekomstige soorten verwerkingen. Hiervoor mogen nadere regels gesteld worden binnen de lijnen van het reglement.

De analyse die uit bovenstaande tekst voortvloeit, is dat de reikwijdte van het reglement, in overeenstemming is met de reikwijdte van de EPV. Dit betekent dus dat de bepalingen van de EPV van toepassing zijn op het privacyreglement. De reikwijdte in het privacyreglement behoeft geen aanpassingen.

8.3.3 Doelstelling voor gegevensverwerking

Uit de theorie blijkt dat de verwerking alleen rechtmatig is indien en voor zover aan ten minste aan bepaalde voorwaarden is voldaan. De verwerking is rechtmatig als; de verwerking noodzakelijk is voor de uitvoering van een overeenkomst, de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die de verantwoordelijke heeft, de verwerking noodzakelijk is om de vitale belangen van een persoon te beschermen, de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang of de uitoefening van het openbaar gezag dat aan de verantwoordelijke is opgedragen en als de verwerking noodzakelijk is voor de behartiging van de gerechtvaardigde

belangen van de verwerkingsverantwoordelijke of van een derde, tenzij de belangen van de betrokkene zwaarder wegen dan die belangen.

In het reglement dat geldend is in de praktijk zijn algemene doelstellingen opgenomen. De persoonsgegevens van medewerkers mogen alleen worden verwerkt indien de organisatie één van deze doelstellingen voor ogen heeft. Deze doelstelling worden opgesteld door de Raad van Bestuur met instemming van de OR. Onverminderd deze doelstellingen mogen persoonsgegevens van medewerkers alleen verwerkt worden indien aan de volgende voorwaarden is voldaan. De Raad van Bestuur is er daarnaast verantwoordelijk voor dat bij elke verwerking bepaalde normen in acht moeten worden genomen. Daarnaast staat in dit artikel dat bijzondere persoonsgegevens binnen het UMCG alleen verwerkt mogen worden als de Wbp dit toestaat, de betrokkene ondubbelzinnig toestemming heeft gegeven voor de verwerking, de persoonsgevens door de betrokkene zelf duidelijk openbaar zijn gemaakt, de verwerking noodzakelijk is voor een recht in rechte of volkenrechtelijke verplichting.

De analyse die uit bovenstaande tekst voortvloeit, is dat de bepalingen met betrekking tot de doelstellingen uit de theorie terugkomen in de praktijk. Het UMCG heeft in het privacyreglement uitgebreid haar doelstellingen, voorwaarden en normen betreffende de gegevensverwerking geformuleerd. Dit voldoet aan de bepalingen van de EPV. Ook hier in het reglement komt de toestemming van de betrokkene weer terug. Toestemming van de medewerker is geen gegarandeerde voorwaarde voor een rechtmatige verwerking van persoonsgegevens van een medewerker.

8.3.4 Bewaartermijnen

Uit de theorie blijkt dat de organisatie ervoor moet zorgen dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is. De verantwoordelijke moet termijnen vaststellen voor het wissen van gegevens en voor een periodieke toetsing hiervan.

Volgens het reglement dat geldend is in de praktijk mogen persoonsgegevens van een medewerkers die uit dienst zijn, tot twee jaar na uitdiensttreding bewaard blijven. Na deze twee jaren moeten de gegevens zo spoedig als redelijkerwijs mogelijk is verwijderd worden.

De analyse die uit bovenstaande tekst voortvloeit, is dat de persoonsgegevens van medewerkers alleen worden verwijderd als een persoon uit dienst treedt. Echter blijkt uit de theorie dat de persoonsgegevens niet langer bewaard mogen worden dan noodzakelijk is. Er is in het reglement niet geformuleerd waarom het twee jaar bewaren van gegevens van medewerkers die uit dienst zijn noodzakelijk is. Daarnaast komt in het reglement niet terug dat er sprake is van een periodieke toetsing of persoonsgegevens verwijderd moeten worden.

8.3.5 Verplichtingen organisatie

Uit de theorie blijkt dat het UMCG als organisatie verschillende verplichtingen heeft als het gaat om de verwerking van persoonsgegevens. Allereerst is de organisatie verplicht om alle rechten van de betrokkenen te faciliteren. Tevens is er de verplichting om actief privacybeleid te gaan voeren nieuw in de EPV. Ook is de verantwoordelijke verplicht passende technische en organisatorische maatregelen te treffen die voldoen aan privacy by design en privacy by default. De organisatie moet hierbij rekening houden met de techniek, de uitvoeringskosten, de aard, de omvang, de context, het doel van de verwerking, de risico's, alsook met de rechten en vrijheden van natuurlijke personen. Ook is de organisatie verplicht dit te evalueren en actualiseren. De documentatieplicht in het Register van de verwerkingsactiviteiten dient te worden opgenomen in het privacyreglement.

In het reglement dat geldend is in de praktijk is de informatieplicht opgenomen. Verder staat er onder de informatieplicht dat gemeld moet worden bij de privacy officer indien er gegevens verwerkt worden op grond van andere doelstellingen dan genoemd in reglement. De documentatieplicht in

het Register van de verwerkingsactiviteiten is opgenomen in het privacyreglement. Er staat namelijk dat de Raad van Bestuur een document dient bij te houden met het specifieke doel van de verwerking, een beschrijving van de opzet van de verwerking, de categorieën medewerkers, aan welke personen of instanties de persoonsgegevens verstrekt zouden kunnen worden, de beveiligingsmaatregelen en de rollen van de FG en de security privacy officer met betrekking tot de persoonsgegevensverwerking. De Raad van Bestuur moet daarnaast op grond van het reglement passende technische en organisatorische maatregelen treffen om de persoonsgegevens te beveiligen.

De analyse die uit bovenstaande tekst voortvloeit, is dat de organisatie nu beperkt haar verplichtingen in het privacybeleid weergeeft. Niet alle rechten van de betrokkenen zijn gefaciliteerd in het privacyreglement. Op dit moment staat er in het reglement dat er passende technische en organisatorische maatregelen getroffen moeten worden om de persoonsgegevens te beveiligen. De bedoeling is dat er bij het treffen van technische en organisatorische maatregelen rekening gehouden wordt met de techniek, de uitvoeringskosten, de aard, de omvang, de context, het doel van de verwerking, de risico's, alsook met de rechten en vrijheden van natuurlijke personen. Dit moet meegenomen worden bij het bepalen van de middelen van verwerken en bij de verwerking zelf. Er wordt niet voldaan aan privacy by design en privacy by default. De documentatieplicht in het Register mist in het privacyreglement.

8.3.6 Rechten betrokkenen

Uit de theorie blijkt dat betrokkenen verschillende rechten hebben op grond van de EPV. Deze rechten zijn als volgt; het recht van bezwaar, het recht op rectificatie, het recht op wissing en afscherming van gegevens, het recht tot inzage en het recht op beperking van de verwerking. De betrokken personen moeten bewust worden gemaakt van de risico's, regels, waarborgen en rechten in verband met de verwerking van persoonsgegevens en van de wijze waarop zij deze rechten kunnen uitoefenen.

In het reglement dat geldend is in de praktijk staat allereerst het recht op inzage vermeld. Daarnaast heeft elke medewerker het recht op correctie of op afscherming van de persoonsgegevens. De privacy officer neemt binnen vier weken beslissing op het verzoek tot wijziging en/of afscherming. Als een medewerker het niet eens is met de beslissing op het verzoek tot inzage, wijziging, verbetering of aanvulling, kan deze een bezwaarschrift indienen bij de Raad van Bestuur. Binnen zes weken wordt hierop beslist. Indien de medewerker het hier niet mee eens is kan deze naar de bestuursrechter gaan. Ook kan de medewerker zich melden bij de AP. Het recht van bezwaar staat vermeld in het artikel over rechtsbescherming.

De analyse die uit bovenstaande tekst voortvloeit, is dat er in het reglement een aantal rechten van betrokkenen zijn opgenomen. Hierbij is vaak ook de wijze waarop de betrokkenen hun rechten kunnen uitoefenen vermeld en hoe hier door de organisatie mee om wordt gegaan. Er zijn echter ook enkele rechten die ontbreken. Dit zijn de rechten die nieuw zijn met de komst van de EPV, namelijk; het recht op wissing en afscherming van gegevens en het recht op beperking van de verwerking. Het recht van bezwaar is in het privacybeleid in een apart artikel opgenomen, namelijk onder het artikel over rechtsbescherming.

8.3.7 Incidenten met betrekking tot persoonsgegevens

Uit de theorie blijkt dat indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, de verwerkingsverantwoordelijke deze binnen 72 uur nadat hij er kennis van heeft genomen dient te melden aan de AP, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Belangrijk is om te regelen hoe de taken verdeeld zijn. Dit allen dient vermeld te worden in het privacybeleid. De

verwerkingsverantwoordelijke dient alle inbreuken in verband met persoonsgegevens te documenteren.

In het reglement dat geldend is in de praktijk is niets geregeld over incidenten met betrekking tot persoonsgegevens.

De analyse die uit bovenstaande tekst voortvloeit, is dat de organisatie de incidenten met betrekking tot persoonsgegevens niet goed geregeld heeft in het privacyreglement. Er wordt in het huidige privacy reglement namelijk helemaal geen aandacht besteed aan incidenten met betrekking tot persoonsgegevens.

8.3.8 Rechtsbescherming

Uit de theorie blijkt dat de betrokkene als rechtsbescherming het recht heeft om in bezwaar te gaan tegen de gegevensverwerking. De verwerkingsverantwoordelijke moet regelingen treffen om de betrokkene in staat te stellen om dit recht van bezwaar uit te oefenen. Het recht van bezwaar moet ook langs de elektronische weg kunnen worden uitgeoefend. De verantwoordelijke moet onverwijld en ten laatste binnen een maand op het verzoek van de betrokkene reageren.

Uit het reglement dat geldend is in de praktijk blijkt dat als een medewerker het niet eens is met een beslissing op een verzoek tot inzage, een beslissing tot afwijzing van het verzoek tot correctie, afscherming, verbetering of aanvulling van persoonsgegevens of een beslissing naar aanleiding van een aantekening van verzet kan deze een bezwaarschrift indienen bij de Raad van Bestuur.

De analyse die uit bovenstaande tekst voortvloeit, is dat de verwerkingsverantwoordelijke in de praktijk in het reglement heeft geregeld dat een betrokkene in bezwaar kan gaan. Dit wordt echter verzet genoemd. Verzet is een term uit de Wbp, welke in de EPV vervangen is door bezwaar. Er staat niet in het reglement dat dit ook elektronisch kan of binnen een maand.

8.3.9 Taalgebruik, toegankelijkheid en formulering

Uit de theorie blijkt dat informatie en communicatie in verband met de verwerking van persoonsgegevens eenvoudig toegankelijk en begrijpelijk dient te zijn. Er en moet duidelijke en eenvoudige taal worden gebruikt. Dit is ook van toepassing op het privacybeleid. Het taalgebruik moet afgestemd zijn op de betrokkene, de medewerker. Deze heeft (vaak) geen juridische achtergrond.

Het reglement dat geldend is in de praktijk is afgestemd op de medewerker geschreven. Duidelijk te zien is dat de rechten van de betrokkenen, welke erg van belang zijn voor de medewerker, in begrijpelijke niet-juridische taal is geschreven. Verder staan er in het privacyreglement wel enkele juridische termen die voor de leek misschien niet eenvoudig zijn, zoals bijvoorbeeld volkenrechtelijke verplichting en publiekrechtelijke taak.

De analyse die uit bovenstaande tekst voortvloeit, is dat het taalgebruik in het privacyreglement deels afgestemd is op de betrokkene. Uit de theorie blijkt dat alle documentatie en communicatie omtrent gegevensbescherming eenvoudig en begrijpelijk dient te zijn.

9. Conclusie en aanbevelingen

Door het analyseren van de verkregen informatie uit het literatuuronderzoek en het praktijkonderzoek kan er een antwoord gegeven worden op de centrale onderzoeksvraag. Het antwoord op de centrale onderzoeksvraag wordt gevormd door de conclusie en aanbevelingen. De doelstelling van het onderzoek is hiermee behaald.
De centrale onderzoeksvraag luidt als volgt:
Op welke manier kan het privacybeleid, toegespitst op de afdeling personeelszaken, van het UMCG worden ingericht, zodat deze compliant is aan de bepalingen van de EPV?

9.1 Conclusie

De conclusies die getrokken kunnen worden na vergelijking van de theorie met de praktijk zijn als volgt:
Op de afdeling P&O is er een UMCG-breed privacyreglement geldend. Het privacyreglement is opgesteld aan de hand van de bepalingen in de Wet bescherming persoonsgegevens (Wbp). Weinig personeelsleden hebben weet van het reglement. Het privacyreglement wordt op dit moment ondergesneeuwd door andere documenten en werkzaamheden.

Met de komst van de Europese Privacy Verordening (EPV) is het vastleggen van de manier waarop met gegevensverwerking en privacy wordt omgegaan binnen organisaties in een privacybeleid verplicht gesteld. Naast het verplichte privacybeleid staan er in de EPV nog meer nieuwe of aangepaste bepalingen. Deze bepalingen geven de regelgeving omtrent het verwerken van persoonsgegevens. Er is ruimte gegeven aan organisaties om het privacybeleid in te richten naar maatstaven die afgestemd zijn op de organisatie, maar tegelijkertijd ook aan de bepalingen van de EPV voldoen.

Op grond van de EPV zijn er de volgende verplichtingen omtrent gegevensverwerking:
Allereerst dient het privacybeleid transparant, beknopt en toegankelijk zijn voor de betrokken partijen. Het beleid moet geschreven zijn in duidelijke en eenvoudige taal, afgestemd op de betrokken partijen. Veelal zullen de persoonsgegevens van de medewerkers verwerkt worden omdat dit noodzakelijk is op grond van de arbeidsovereenkomst. Dit moet vermeld worden in het privacybeleid. Er moet tijdens het stellen van maatregelen in bijzonder rekening gehouden worden met privacy by design en default. De bescherming van de persoonsgegevens moet vanaf de eerste fase namelijk gewaarborgd zijn. Achteraf moet het UMCG kunnen verantwoorden dat zij dit heeft gedaan. In het privacybeleid moeten de rechten van betrokkenen en de verplichtingen van de organisatie terugkomen. Tevens mogen de persoonsgevens niet langer worden bewaard dan noodzakelijk is voor de doeleinden waarvoor zij zijn bewaard.

Het privacybeleid dient goed geïmplementeerd worden binnen de organisatie. De manier waarop het UMCG dit wil gaan doen dient verwerkt te worden in het privacybeleid. Alle medewerkers moeten in overeenstemming met het privacybeleid handelen. De verantwoordelijkheid dat een privacybeleid goed werkt in de praktijk, ligt te allen tijde bij de organisatie. Bij de implementatie dienen de belangen die verschillende partijen binnen (de afdeling P&O van) het UMCG hebben bij een goed ingericht privacybeleid meegenomen te worden;
- Het UMCG wil als organisatie een goede band met haar medewerkers onderhouden. Deze band kan aangetast worden indien zij niet transparant en vertrouwelijk met personele data omgaat. Daarnaast is het de taak van het UMCG om in overeenstemming met wet- en regelgeving te handelen. Hiermee hangt samen dat het UMCG imagoschade en bestuurlijke boetes wil voorkomen.
- De medewerkers hebben allereerst het belang dat er zorgvuldig en vertrouwelijk met hun persoonsgegevens wordt omgegaan. Daarnaast zijn er medewerkers die de personele data verwerken. Deze partij heeft belang bij een laagdrempelig, eenvoudig toegankelijk en geconcretiseerd privacybeleid, waardoor zij hun werkzaamheden goed uit kunnen voeren.

9.2 Aanbevelingen

Met de komst van de EPV verdienen twee hoofdlijnen aandacht van organisaties met betrekking tot het privacybeleid. Allereerst dient het privacybeleid compliant aan de bepalingen van de EPV te zijn. Daarnaast moet het privacybeleid nageleefd worden op de werkvloer. Een EPV-compliant privacyreglement waar achteraf weinig mee gedaan wordt binnen de organisatie, heeft namelijk als gevolg dat de organisatie nog steeds niet EPV-compliant is. Met het opstellen van de aanbevelingen zijn de belangen van het UMCG als organisatie en van de medewerkers in acht genomen.

Hoofdlijn 1

Om te zorgen dat het huidige privacyreglement compliant is aan de bepalingen van de EPV, moeten er een aantal aanpassingen gedaan worden. Aanbevolen wordt om de volgende wijzigingen aan te brengen in het huidige privacyreglement om te komen tot een goed privacybeleid:

- In het beginstuk over de achtergrond van het reglement dient beschreven te worden dat de EPV de regels geeft ter bescherming van de persoonlijke levenssfeer in verband met de verwerking van persoonsgegevens. De andere wetgeving die aangehaald wordt in het reglement, zoals de Wet op de Ondernemingsraden en de Archiefwet dienen hun plek te behouden.

- In de begripsbepalingen dienen er een aantal wijzigingen doorgevoerd te worden. Allereerst dient toegevoegd te worden wanneer er sprake is van een 'bijzonder persoonsgegeven'. Op dit moment komt dit pas terug bij de doelstellingen. Tevens moet toegevoegd worden wat pseudonimisering, beperken van de verwerking, inbreuk in verband met persoonsgegevens en gegevens over gezondheid inhouden.

- Aanbevolen wordt om de 'verantwoordelijke' vervangen te worden door de 'verwerkingsverantwoordelijke'. Het begrip de 'bewerker' dient vervangen te worden door de 'verwerker'. De definities hiervan kunnen overgenomen worden uit de begripsbepaling van de EPV.

- Enkele begrippen zijn in definitie veranderd, namelijk: persoonsgegevens, betrokkene, verwerking, bijzondere persoonsgegevens en verwerker. De definities hiervan kunnen overgenomen worden uit de begripsbepaling van de EPV.

- Het begrip toestemming van betrokkene kan mijns inziens het beste verwijderd worden uit de begripsbepalingen, omdat toestemming van betrokkene geen gegarandeerde voorwaarde is voor een rechtmatige verwerking van persoonsgegevens van medewerkers. De andere niet-behandelde begrippen kunnen blijven staan.

- Aanbevolen wordt om de uitgangspunten van het UMCG toe te voegen aan het reglement, die te lezen zijn in het kaderbeleid (bijlage 1). Hierdoor is duidelijk van welke aannames en veronderstellingen het UMCG uitgaat als organisatie. Dit heeft verduidelijking van de achtergrond achter (bepaalde) artikelen tot gevolg.

- Aanbevolen kan worden om een nieuw artikel toe te voegen aan het reglement, genaamd: rollen en verantwoordelijkheden. Op dit moment worden de rollen en verantwoordelijkheden van de verschillende partijen door het hele reglement heen beschreven. Op deze manier is niet overzichtelijk wie wat moet doen. De rol van de Raad van Bestuur is erg groot volgens het reglement. Misschien worden enkele taken op dit moment al vervangen door de Privacy werkorganisatie, een FG of een privacy officer. Van belang is om te bepalen of de Raad van Bestuur deze taken uitvoert, op welke wijze en of de taken ook aan anderen toebedeelt moeten

worden. Hieronder kan ook beschreven worden wie de verplichtingen, zoals de documentatieplicht, op zich zal nemen.

- Het artikel betreffende de bewaartermijnen behoeft niet veel verandering. Op dit moment worden de persoonsgegevens van uit dienst getreden medewerkers twee jaar bewaard. De gegevens mogen bewaard worden zolang dit noodzakelijk is voor doeleinden waarvoor deze zijn bewaard. Aanbevolen kan worden om hier niet een standaardtermijn van twee jaar te hanteren, maar een maximale bewaartermijn van twee jaar. De gegevens zullen nu mogelijk langer bewaard worden dan noodzakelijk.

- Aanbevolen wordt om een nieuw artikel betreffende de verwerking van persoonsgegevens toe te voegen. Dit artikel dient rechtstreeks in te gaan op alle aspecten van het verwerken. Allereerst dient hier uitgewerkt te worden hoe de organisatie privacy by design en privacy by default in acht wil gaan nemen. Daarnaast moet de grondslag, doelbinding en de wijze van belangenafweging omschreven worden.

- Het taalgebruik van het privacyreglement is deels afgestemd op de betrokkene. Er worden echter nog enkele juridische begrippen gehanteerd. Aanbevolen wordt om het privacyreglement zo eenvoudig mogelijk te beschrijven. Hier is enigszins winst te behalen voor het UMCG.

- Aanbevolen kan worden om in het privacybeleid op te nemen welke informatie omtrent ziekteverzuim verwerkt mag worden. Hierbij moeten de beleidsregels van de AP in acht worden genomen.

- Raadzaam is om een apart artikel op te nemen omtrent de evaluatie van de verwerkingen van persoonsgegevens. Hierin kan omschreven worden wanneer er geëvalueerd wordt en welke partijen hier aanwezig zijn. Dit zorgt ervoor dat partijen zich moeten verantwoorden, waardoor zij zich sneller aan het privacybeleid zullen houden.

- Er dient tevens een apart artikel opgenomen te worden omtrent datalekken. Dit kan bijvoorbeeld ‘incidenten met betrekking tot persoonsgegevens’ worden genoemd. Op dit moment is hier niets over geregeld. Duidelijk omschreven moet worden wanneer er sprake is van een datalek, waar dit gemeld moet worden, wie dit doet en hoe dit verder afgehandeld wordt.

- De rechten van inzage en het recht op correctie en afscherming zijn op dit moment correct in het reglement opgenomen. Het recht op beperking van de verwerking ontbreekt hier en aanbevolen wordt om deze toe te voegen. Aanbevolen wordt om het recht op afscherming uit te breiden met het recht op wissing. De verwerkingsverantwoordelijke moet namelijk redelijke maatregelen treffen om andere gegevensverwerkers ervan op de hoogte te stellen dat de betrokkene wil dat zijn of haar gegevens verwijderd worden. Het UMCG is verplicht om al deze rechten correct te faciliteren.

- Aanbevolen wordt om een PIA, oftewel een gegevensbeschermingseffectbeoordeling uit te (laten) voeren. Hierdoor kunnen de risico’s die het UMCG loopt vooraf in kaart worden gebracht.

Hoofdlijn 2

Aanbevelingen voor compliance en implementatie van het privacybeleid op de werkvloer zijn:

- Een vorm van bewustwording kan verwezenlijkt worden door aan de medewerkers duidelijk te maken waarom er verandering plaatsvindt. De respondenten hebben verschillende opties gegeven hoe zij denken dat dit bereikt kan worden, namelijk; het actueel maken dat andere bedrijven boetes hebben gekregen, het laten zien van filmpjes waarin individuen geschaad zijn omdat er niet goed is omgegaan met privacygevoelige informatie en posters op de afdeling.

- Aanbevolen worden om per werkzaamheid duidelijk in kaart te brengen wat de veranderingen zijn. Dit heeft als gevolg dat de medewerkers niet zelf uit hoeven te zoeken welke bepalingen allemaal op hun werkzaamheden van toepassing zijn.

- Aanbevolen wordt om ervoor te zorgen dat er een waarschuwing in het scherm verschijnt indien een personeelslid in personeelsdata zit. Tevens wordt aanbevolen om een waarschuwing te laten verschijnen indien een personeelslid in personeelsdata zit maar daar al een tijd niets in heeft gedaan.

- Aanbevolen wordt om de vindbaarheid van het privacybeleid laagdrempelig te houden. Het privacybeleid dient zo toegankelijk mogelijk te zijn. Dit kan verwezenlijkt worden door het privacybeleid naar alle medewerkers te mailen, het privacybeleid een eigen kopje te geven op het intranet en door het privacybeleid uitgeprint te verstrekken aan medewerkers.

- Aanbevolen wordt om tijdens de voorbereidingen op de implementatie van het nieuwe privacybeleid in het achterhoofd te houden dat het huidige privacyreglement niet goed geïmplementeerd is op de werkvloer van de afdeling P&O. Raadzaam is om te evalueren wat er precies misgegaan is tijdens de vorige implementatie en hoe dit anders kan. Aanbevolen wordt om hiervoor de stappen uit hoofdstuk 6 te volgen.

Literatuurlijst

Berkvens 2002
J.M.A. Berkvens & J.E.J. Prins, *Recht en Praktijk: Privacyregulering in theorie en praktijk*, Deventer: Kluwer 2002.

Bleker 2010
S. C. Bleker-van Eyk, 'Het belang van compliance voor ziekenhuizen', *VU Magazine, Compliance & Integriteit*, nr 3, december 2010.

CBP 2001
CBP*, De Wet Bescherming Persoonsgegevens*. *Over de bescherming van uw persoonlijke gegevens*, Den Haag: Sdu Grafische Bedrijven 2001.

De Jong 2015
J.P. de Jong, 'De Algemene verordening gegevensbescherming. De rechtsopvolger van de Wbp', *Regelmaat* 2015.

Duthler 2013
Mr. Dr. A.W. Duthler & Drs. A.J. Biesheuvel, *Het Europees privacyrecht in beweging*, Deventer: Kluwer 2013.

Grit 2009
R. Grit en M. Gerritsma, *Zo maak je een beleidsplan*, Noordhof uitgevers: Groningen: 2009.

Hustinx 2002
P.J. Hustinx, *Bewerkers en verantwoordelijke: de relatie nader toegelicht,* Den Haag: CBP 2002.

NVZ 2014
'Nieuwe privacyregels in aantocht', *NVZ* 23 mei 2014, www.nvz-ziekenhuizen.nl *(*zoek op *Nieuwe privacyregels in aantocht*).

Right Marktonderzoek 2016
'Methoden onderzoek, kwalitatief onderzoek', *Rightmarktonderzoek*, www.rightmarktonderzoek.nl, (klik op *methoden onderzoek, kwalitatief onderzoek*).

Steffin 2014
M. Steffin, E. Zaaiman, A. de Bruijn, *Bescherming van persoonsgegevens, Spotlight,* Jaargang 21 - 2014 uitgave 3.

Van der Wijst 2014
'Nieuwe EU privacyverordening', www.bgadvocaten.nl, *BGA*, (zoek op *nieuwe EU privacyverordening*), 2014.

Van Leeuwen 2009
B.H.A. van Leeuwen, A.G.H. van der Staay & O. Javornik, *Beroep: bedrijfsjurist, Praktische leidraad voor bedrijfsjuristen*, Deventer: Kluwer, 2009.

Van Lieshout 2012
M. van Lieshout, *Stimulerende en remmende factoren van Privacy by Design*, Delft: TNO 2012.

Van Oosterhout 2015
A. van Oosterhout, *Europese privacyverordening: de stand van zaken,* Twinkle Magazine, 2015.

Verschuren 1995
P. Verschuren, H. Doorewaard, *Het ontwerpen van een onderzoek*, Utrecht: Lemma 1995.

WODC 2007
G. J. Zwenne, A.W. Duthler, M. Groothuis, H. Kielman, W. Koelewijn, L. Mommers, *Eerste fase evaluatie Wet bescherming persoonsgegevens,* Leiden*:* WODC 2007.

WODC 2008
H.B. Winter, P.O. de Jong, A. Sibma, F.W. Visser, M. Herweijer, A. M. Klingenberg, H. Prakken, *Wat niet weet, wat niet deert*, Groningen: WODC 2008.

Bijlagen

Bijlage 1. EPV-kaderbeleid UMCG

1. Inleiding: UMCG en privacy

Het UMCG staat voor excellente zorg, onderzoek en onderwijs en opleiding[123]. Het zorgvuldig omgaan met eenieders privacy maakt daar zondermeer onderdeel van uit. Aansluitend bij de waarden en ambities van het UMCG, in het bijzonder op het gebied van kwaliteit en veiligheid, is handelen in overeenstemming met privacy wet- en regelgeving niet alleen een kwestie van moeten, maar veel meer nog een kwestie van willen. Wij vinden het belangrijk om in het UMCG de mens centraal te stellen bij alles wat we doen waarbij veilig, respectvol en betrouwbaar relevante kernwaarden vormen óók als het gaat om privacybescherming.

Dit vormt de basis voor het UMCG om het privacybeleid in haar organisatie vorm en inhoud te geven. Daarenboven heeft het UMCG de wettelijke plicht om privacybeleid vast te stellen op grond van artikel 11 lid 1 en artikel 22 lid 1 Algemene Verordening Gegevensbescherming (AVG)[124].

De aanleiding om anno 2015 kwaliteit van privacybescherming naar een hoger niveau te willen brengen is ingegeven door het feit dat het UMCG verantwoordelijk is voor het verwerken van persoonsgegevens op het gebied van patiëntenzorg, onderzoek, opleiding- en onderwijs en bedrijfsvoering. De omvang van de verwerking van persoonsgegevens van patiënten, medewerkers en deelnemers aan onderzoek is zeer groot. Daar komt bij dat het vaak zeer privacygevoelige gegevens betreffen, zoals gegevens betreffende de gezondheid. Dit benadrukt het belang om als universitair medisch centrum met de grootste mate van zorgvuldigheid, integriteit en betrouwbaarheid met de persoonsgegevens om te gaan. Daarnaast brengen ontwikkelingen op het gebied van wetgeving op zowel Europees, als nationaal niveau, zoals de Algemene Verordening Gegevensbescherming (AVG) - in het spraakgebruik ook vaak aangeduid als Europese Privacy Verordening (EPV) - en de Wet Meldplicht Datalekken[125], verscherpte eisen op het gebied van transparantie en accountability voor de verwerking van persoonsgegevens met zich mee. Het UMCG wil aan de hand van de (nieuwe) privacywetgeving met dit beleid uitgangspunten voor de privacybescherming formuleren en beleidskeuzes nader verantwoorden.

In paragraaf 2 zijn de uitgangspunten van het UMCG Privacybeleid geformuleerd. In paragraaf 3 worden de verantwoordelijkheden en governance als het gaat om het geven van uitvoering aan het Privacybeleid UMCG uitgewerkt. Paragraaf 4 geeft de kaders aan waarbinnen verantwoording kan worden afgelegd over de wijze waarop uitvoering wordt gegeven aan privacy wet- en regelgeving en meer in het bijzonder hoe persoonsgegevens worden verwerkt en beschermd.

2. Uitgangspunten van het Privacybeleid UMCG

Privacy is een breed en ruim begrip. Naast de term persoonlijke levenssfeer komt men in de context van het recht op privacy ook wel de termen persoonlijke levenssfeer, privéleven en eigenruimte tegen, alsook de bescherming van persoonsgegevens. Het omvat het recht op het beschermen van het eigen lichaam, maar ook het recht op vertrouwelijk communiceren. Allemaal aspecten van privacy die in het UMCG relevante onderwerpen zijn in de dagelijkse omgang met elkaar. We hebben allemaal elke dag te maken met privacy.

[123] Bouwen aan de toekomst van gezondheid 2020.

[124] De AVG betreft een wetsvoorstel van de Europese Commissie. Het wetsvoorstel heet voluit het “Voorstel voor een Verordening van het Europees parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens”. Zie ook bijlage 2 bij dit document.

[125] Voor toelichting zie bijlage 2 bij dit document.

Het UMCG legt in dit Privacybeleid UMCG de nadruk op de verwerking en bescherming van persoonsgegevens in het UMCG, zonder daarbij voorbij te willen gaan aan wat privacy in brede zin behelst. Binnen dit gegeven formuleert het UMCG de volgende uitgangspunten ten aanzien van de bescherming van de privacy in het algemeen en het verwerken van persoonsgegevens in het bijzonder:

- Het UMCG verwerkt persoonsgegevens op een wijze die rechtmatig, eerlijk en transparant is;

- Het UMCG verzamelt persoonsgegevens enkel voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen. Het UMCG zal persoonsgegevens niet op een met die doeleinden onverenigbare wijze verwerken;

- Het UMCG heeft de verdeling van verantwoordelijkheden voor de verwerking van de persoonsgegevens binnen haar organisatie duidelijk belegd (zie: paragraaf 3 van dit beleid). De voor de verwerking verantwoordelijke zorgt ervoor en kan aantonen dat elke verwerking voldoet aan de Wet bescherming Persoonsgegevens (Wbp) en de Algemene Verordening Gegevensbescherming (AVG);

- Het UMCG respecteert de rechten van betrokkene. De betrokkene heeft recht op informatie, het recht op toegang (het recht op inzage en afschrift), het recht op rectificatie, het recht om te worden vergeten en om gegevens te laten wissen, het recht op gegevensoverdraagbaarheid (dataportabiliteit) en het recht van bezwaar.

- Het UMCG is verantwoordelijk voor het treffen van passende technische en organisatorische maatregelen met betrekking tot de bescherming van persoonsgegevens. De kwaliteit van het beschermingsniveau wordt evenwel mede bepaald door het gedrag van de medewerkers in het UMCG. Het UMCG wil – gemotiveerd vanuit haar kernwaarden veilig, betrouwbaar en respectvol – medewerkers die door bewust en (pro)actief handelen uitvoering geven aan (de geest van de) privacywetgeving.

De bovengenoemde uitgangspunten zijn algemeen van aard en gelden organisatiebreed. De uitgangspunten zijn nader uitgewerkt in het **Privacy Reglement UMCG**. Het Privacybeleid UMCG en het Privacy Reglement UMCG leggen de basis voor de feitelijke inrichting en kwaliteit van privacybescherming in het UMCG. Een uitwerking van het Privacybeleid UMCG en het Privacy Reglement UMCG in nader beleid, richtlijnen, protocollen en/of werkprocessen dient altijd passend te zijn binnen dit UMCG beleid en het reglement en moet hieraan worden getoetst.

3. Verantwoordelijkheden en governance

De verantwoordelijkheid voor de verdere implementatie van privacybescherming is door de Raad van Bestuur voor de periode van één jaar, tot 1 juni 2016, gemandateerd aan het hoofd Juridische Zaken.

In dit jaar wordt privacybeleid ontwikkeld en vastgesteld en zullen procedures, richtlijnen en codes worden ontwikkeld en herijkt aan de nieuwe privacy wetgeving. Tevens wordt de definitieve positionering van de werkorganisatie voorbereid.

De bescherming van persoonsgegevens heeft directe relatie met informatiebeveiliging. Deze directe relatie wordt gelegd in artikel 13 van de Wbp en artikel 30 AVG waarin de verantwoordelijke voor de verwerking van persoonsgegevens wordt verplicht om passende technische- en organisatorische maatregelen te treffen om persoonsgegevens te beveiligen. Kort gezegd, als het gaat om

privacybescherming dan zijn maatregelen op het gebied van informatiebeveiliging vereist. Het interne informatiebeveilingsbeleid van het UMCG is vastgelegd in het document 'UMCG Informatiebeveiliging 2013-2017'[126]. Het Privacybeleid UMCG sluit zoveel mogelijk aan bij dit informatiebeveilingsbeleid voor zover dit betrekking heeft op de beveiliging van persoonsgegevens.

Om op een geïntegreerde wijze de bescherming en beveiliging van persoonsgegevens conform de normen van de AVG voor te bereiden, is een werkorganisatie privacybescherming opgericht. Deze werkorganisatie is vooralsnog gepositioneerd bij Bureau Juridische Zaken. De werkorganisatie wordt ondersteund en begeleid door een stuurgroep, waarin directeuren en hoofden van betrokken organisatieonderdelen vertegenwoordigd zijn. Het Hoofd Juridische Zaken, tevens voorzitter van de stuurgroep, legt verantwoording af aan de Raad van Bestuur. Binnen de werkorganisatie worden vraagstukken waarbij zowel privacybescherming alsook informatiebeveiliging een rol spelen, zoveel als mogelijk geïntegreerd opgepakt.

3.1 Werkorganisatie privacybescherming

De werkorganisatie privacybescherming en heeft als taak om in- en externe ontwikkelingen op het gebied van privacybescherming, inclusief die op het terrein van wet- en regelgeving, naar UMCG-beleid te vertalen. Binnen de verschillende beleidsterreinen moet privacybescherming, inclusief de bijbehorende technische en organisatorische maatregelen, als onderdeel van beleid worden meegenomen. Het gaat hier in het bijzonder om aspecten die noodzakelijk zijn om het UMCG in overeenstemming met de nieuwe AVG te laten functioneren.

De werkorganisatie heeft de volgende hoofdtaken:

- Het hebben van een ondersteunende- en faciliterende rol bij het creëren van overzicht en inzicht op het gebied van verwerkingen van persoonsgegevens;
- Het integreren van privacy als vast onderdeel van c.q. aandachtspunt binnen de bedrijfsvoering en werkprocessen binnen de gehele organisatie;
- Het faciliteren van Privacy by Design en Default en het uitvoeren van Privacy Impact Assessment (PIA's) als het gaat om nieuwe of substantiële wijzigingen bij het verwerken van persoonsgegevens;
- Het jaarlijks controleren van het beschermingsniveau van de verwerking van persoonsgegevens en hierover te rapporteren.

Daarnaast heeft de werkorganisatie zich ten doel gesteld dat:

- Duidelijk zichtbaar is voor de medewerkers van het UMCG waar specifieke inhoudelijke kennis op het gebied van privacybescherming gebundeld en beschikbaar is;
- Ondersteuning wordt geboden aan de organisatieonderdelen om de privacybescherming en informatiebeveiliging van persoonsgegevens te kunnen optimaliseren.

3.2 Functionaris voor de gegevensbescherming (FG)

De functie van functionaris voor de gegevensbescherming (FG) wordt vervuld vanuit Bureau Juridische Zaken. De FG vervult een rol waar het gaat om informeren en adviseren van de voor de verwerking verantwoordelijke over verplichtingen die voortvloeien uit privacy wet- en regelgeving. De FG houdt toezicht op de naleving van de uit de wet- en regelgeving voortvloeiende eisen en ook

[126] UMCG Informatiebeveiliging 2013-2017 (juni 2013), kenmerk 278.847/RvB.

op de implementatie en toepassing van het privacybeleid. De FG houdt toezicht of de verwerkingen van persoonsgegevens in overeenstemming met wet- en regelgeving worden uitgevoerd. De FG houdt eveneens toezicht op het documenteren en melden van datalekken, de wijze waarop uitvoering wordt gegeven aan de PIA/BIA en de wijze waarop gevolg wordt gegeven aan verzoeken van het College Bescherming Persoonsgegevens (CBP).

De FG houdt toezicht op het register waarin de verschillende meldingsplichtige gegevensverwerkingen en van de door het UMCG gesloten bewerkersovereenkomsten, convenanten en privacy protocollen.

De FG treedt op als contactpersoon voor het CBP en neemt zo nodig op eigen initiatief contact op met het CBP voor zover het noodzakelijk is om het CBP te raadplegen.

De FG rapporteert regulier aan het hoofd Juridische Zaken. In bijzondere situaties is hij gerechtigd rechtstreeks aan de Raad van Bestuur te rapporteren.

3.3 Organisatieonderdelen

De Raad van Bestuur van het UMCG heeft er voor gekozen om taken, verantwoordelijkheden en bevoegdheden zo dicht mogelijk bij de afdelingen te beleggen. Dit geld ook voor de bescherming van persoonsgegevens.

De verantwoordelijkheid voor de uitvoering van het privacybeleid is daarom bij de leidinggevenden van de verschillende afdelingen belegd. Elke leidinggevende is verantwoordelijk voor een zorgvuldige verwerking van persoonsgegevens binnen zijn of haar afdeling en rapporteert hierover in de reguliere PDCA-cyclus. Dit vereist dat leidinggevenden de documenten inzake alle verwerkingen van persoonsgegevens die onder hun verantwoordelijkheid hebben plaatsgevonden bewaren en documenteren (artikel 28 AVG).

4. Verantwoording

Het privacybeleid UMCG is een beleidsstuk dat de kaders geeft waarbinnen - zowel intern als extern - verantwoording kan worden afgelegd over de wijze waarop binnen het UCMG uitvoering wordt gegeven aan privacy wet- en regelgeving en meer in het bijzonder hoe persoonsgegevens worden verwerkt en beschermd.

Om te kunnen toetsen of het UMCG voldoet aan privacy wet- en regelgeving is inzicht en overzicht in de verwerkingen van persoonsgegevens vereist. Met inzicht en overzicht wordt mede vorm en inhoud gegeven aan de documentatieplicht uit artikel 28 AVG. De documentatieplicht vormt tevens de basis om het kunnen voldoen aan de rechten van betrokkene.

Het voldoen aan de vereisten vanuit de wet- en regelgeving, waaronder met name de AVG, Wbp en de Meldplicht datalekken, wordt middels audits getoetst door de FG. Jaarlijks wordt het resultaat van de PDCA-cyclus gerapporteerd aan het hoofd Juridische Zaken en de Raad van Bestuur. In het kader van de certificering ISO9001 en ISO 27001 is privacybescherming een onderdeel van de externe kwaliteitsaudits van DNV.

Gebruikte afkortingen:

AVG	: Algemene Verordening Gegevensbescherming
FG	: Functionaris voor de gegevensbescherming
CBP	: College Bescherming Persoonsgegevens
Wbp	: Wet Bescherming persoonsgegevens
PIA	: Privacy Impact Assessment
BIA	: Business Impact Assessment
PDCA-cyclus	: Plan-Do-Check-Act-cyclus

Privacy by design	: Privacy by design betekent dat al in de voorfase van een (ICT-) project – al vanaf het ontwerp – wordt gekeken naar technische en organisatorische maatregelen die privacyverhogend zijn. In plaats van de wet toe te passen op het te ontwikkelen systeem, wordt de wet in het systeem ingebouwd. Privacy by design omvat een aan de bouw van systemen, diensten en netwerken voorafgaande privacyrisico- of privacybedreigingsanalyse (privacy impactanalyse) en een management cyclus binnen organisaties waar privacybescherming een vast onderdeel is.
Privacy by default	: Privacy by default lijkt op het privacy by design principe en betekent dat door middel van systeeminstellingen maximale privacy van een betrokkene wordt gewaarborgd en voor zover mogelijk door het systeem wordt afgedwongen.

Relevante wetgeving:

- Europees Verdrag voor de rechten van de mens (EVRM);
- Grondwet (GW);
- Wet bescherming persoonsgegevens (Wbp);
- Algemene Verordening Gegevensbescherming (AVG) (wetsvoorstel)
- Wet meldplicht datalekken en uitbreiding bestuurlijke boetebevoegdheid CBP;
- Wet op de geneeskundige behandelingsovereenkomst (WGBO);
- Wetsvoorstel kwaliteit, klachten en geschillen zorg.
- Wetsvoorstel cliëntenrechten bij elektronische verwerking van gegevens.

Daar waar het in het Privacybeleid UMCG gaat om privacy wet- en regelgeving wordt primair bedoeld de AVG, Wbp en de Wet meldplicht datalekken.

In het beleid is de afkorting AVG aangehouden, omdat dit de officiële afkorting is die de Europese Commissie aan het wetsvoorstel heeft gegeven. Het wetsvoorstel heet voluit het “Voorstel voor een Verordening van het Europees parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens”. In de praktijk wordt het wetvoorstel vaak de Europese Privacy Verordening genoemd.

Ten tijde van het schrijven van het Privacybeleid UMCG is de Wbp geldend recht. Daar waar het privacy aangaat, moet het UMCG voldoen aan deze wet. De AVG is een Europese verordening die nog in voorbereiding is. De eisen vanuit deze verordening die aan de verwerking van persoonsgegevens wordt opgelegd zijn op onderdelen strenger. In de verordening worden sancties gekoppeld aan het niet-naleven van de verordening, waaronder de sanctie tot het opleggen van een bestuurlijke boete.

De wet meldplicht datalekken is op 26 mei 2015 door de Eerste Kamer aangenomen. De wet treed in werking met ingang van 1 januari 2016. De verplichting tot het melden van datalekken door verantwoordelijken en bewerkers wordt geregeld door aanvullende bepalingen op te nemen in de Wet bescherming persoonsgegevens (Wbp) en de Telecommunicatiewet (Tw).

Bijlage 2. Beleidsregels ziekteverzuim

Enkele belangrijke beleidsregels worden hieronder weergegeven:

1. De sollicitatieprocedure[127]:

- De werkgever mag bij een sollicitatie niet vragen naar de gezondheid van de sollicitant of het eerdere ziekteverzuim van de sollicitant. De sollicitant is verplicht medische informatie mee te delen indien deze ertoe leiden dat hij of zij mogelijk ongeschikt is voor de functie waarop de sollicitatie berust.

- De werkgever mag alleen van de sollicitant eisen dat hij of zij een aanstellingskeuring door de bedrijfsarts ondergaat indien de functie waarop gesolliciteerd wordt bijzondere eisen stelt aan de medische conditie van de sollicitant. Voorbeeld hiervan is als er gesolliciteerd wordt op een functie in het leger. Er worden alleen medische aspecten onderzocht die noodzakelijk zijn voor de functie waarop gesolliciteerd wordt. De sollicitant kan te allen tijde weigeren dat de bedrijfsarts de uitslag bekend maakt, en deze mag dat dan alleen doen in de termen; 'geschikt (onder voorwaarden)' en 'ongeschikt'.

- De werkgever mag niet vragen of de sollicitante zwanger is of in de toekomst kinderen zou willen krijgen. Indien de werkgever dit wel vraagt, hoeft de sollicitante niet van een eerlijk antwoord te voorzien.

2. Bij ziekmelding[128]

- Bij ziekmelding van de werknemer mag de werkgever alleen de volgende gegevens van de werknemer vragen en registreren;

  1. Het telefoonnummer en (verpleeg)adres van de werknemer.
  2. De vermoedelijke duur van het verzuim.
  3. De lopende afspraken en werkzaamheden van de werknemer.
  4. Of de werknemer onder een van de bepalingen van de Ziektewet valt.
  5. Of de ziekte verband houdt met een arbeidsongeval.
  6. Of er sprake is van een verkeersongeval waarbij een eventueel aansprakelijke derde betrokken is. Dit laatste in verband met regresmogelijkheid van de werkgever[129].

- De werkgever mag geen andere gegevens over de medische toestand aan de werknemer vragen. De werknemer kan zich namelijk op grond van de arbeidsrelatie verplicht voelen om deze gegevens mee te delen, waardoor er geen sprake is van vrije wil. De vrije wil is, zoals hierboven besproken, een vereiste om met toestemming persoonsgegevens van werknemers te vragen en te registreren. Echter, in de EPV is opgenomen dat toestemming van een werknemer nooit een rechtsgrondslag is voor het verwerken van zijn of haar persoonsgegevens.

- De werkgever mag wel vrijwillig verstrekte medische gegevens van de zieke werknemer registreren indien dit noodzakelijk is. Voorbeelden hiervan zijn epilepsie. Collega's en de werkgever zelf kunnen bij een epileptische aanval dan handelen naar de situatie.

3. Ziekteverzuimbegeleiding en re-integratie[130]

- Indien er sprake is van langdurige ziekte wordt er vaak een bedrijfsarts ingeschakeld. De bedrijfsarts heeft, ondanks dat deze werkt voor de werkgever, een geheimhoudingsplicht.

[127] AP, *De zieke werknemer en privacy. Regels voor de verwerking van persoonsgegevens van zieke werknemers*, april 2016, p. 17 en 18
[128] Idem, p. 19
[129] artikel 6:107a, lid 2 BW
[130] AP, *De zieke werknemer en privacy. Regels voor de verwerking van persoonsgegevens van zieke werknemers*, april 2016, p. 5 en 6.

De bedrijfsarts mag dus niet zomaar informatie over de ziekte van de werknemer verschaffen aan de werkgever. Met betrekking tot het verschaffen van medische gegevens van de zieke werknemer is de bedrijfsarts strikt aan regels gebonden.

- Er zijn enkele punten die de bedrijfsarts wel bekend mag maken aan de werkgever, namelijk;
  1. Welke taken op het werk de werknemer wel en niet kan uitvoeren.
  2. Hoelang de bedrijfsarts verwacht dat het ziekteverzuim aan zal houden.
  3. De mate waarin de werknemer arbeidsongeschikt is.
  4. Adviezen over aanpassingen of werkvoorzieningen die de werkgever moet verzorgen voor het integratieproces.

- De bedrijfsarts dient aan het UWV de medische gegevens van de werknemer te verstrekken, welke het UWV nodig heeft om haar taken correct uit te kunnen voeren.

- Het kan zo zijn dat een andere werknemer de taak krijgt om ziekteverzuimbegeleiding te geven. Dit is een opdracht van de bedrijfsarts. De werknemer die deze taken uitvoert mag wel over de medische gegevens van de zieke werknemer beschikken als dit noodzakelijk is voor een goede uitvoer van de ziekteverzuimbegeleiding. Dit is echter alleen zo als de bedrijfsarts zijn taken 'echt' delegeert aan de werknemer. Indien de werknemer alleen zorgt voor coördinatie en faciliteiten, hoeft deze de medische gegevens niet te weten.

- De gegevens die de bedrijfsarts aan de werkgever moet verstrekken, mag de werkgever verwerken.

4. Verzekeraars

- Indien de verzekeraar moet beoordelen of een aanspraak rechtvaardig is, moet deze kunnen beschikken over bepaalde gegevens. De werkgever is dan ook verplicht om de volgende gegevens over de zieke werknemer aan de verzuimverzekeraar te verschaffen;
  1. De NAW-gegevens van de zieke werknemer

  2. De hoogte van de loon van de zieke werknemer
  3. De datum van de eerste ziektedag
  4. De datum waarop de werknemer vermoedelijk hersteld is
  5. De vermoedelijke duur van het verzuim
  6. Het arbeidsongeschiktheidspercentage of de door de werkgever vastgestelde loonwaarde;
  7. Het aantal uren dat de werknemer zijn eigen werk of passend werk kan doen
  8. Of de werkgever enige vergoeding heeft ontvangen voor de zieke werknemer
  9. Of het loon aan de werknemer doorbetaald wordt
  10. Of en wanneer een interventie is ingezet
  11. Of er een plan van aanpak is opgesteld
  12. Of de activiteiten uit het plan van aanpak worden uitgevoerd
  13. Of de re-integratie tijdig van start gaat

5. Verzuimsystemen[131]

- Het systeem waarin de gegevens omtrent zieke werknemers opgeslagen worden moeten aan bepaalde vereisten voldoen. De risico's met betrekking tot de beveiliging moeten op vaste tijd terugkerend gepeild worden.

- De wachtwoorden die op verzuimsystemen zitten moeten bestaan uit twee factoren. Te denken valt aan het inloggen op internetsite van een bank. Dit wordt een twee-authenticatie wachtwoord genoemd.

[131] AP, *De zieke werknemer en privacy. Regels voor de verwerking van persoonsgegevens van zieke werknemers*, april 2016, p. 32 en 33

6. Bewaartermijnen[132]

- De gegevens die betrekking hebben op de ziekte van de werknemer mogen niet langer bewaard worden dan noodzakelijk is voor het doel waarvoor deze in eerste instantie zijn opgeslagen.
- Indien de werknemer niet meer in dienst is bij de werkgever, mag de werkgever zijn gegevens hoogstens tot twee jaar na uitdiensttreding bewaren. Indien de werkgever eigenrisicodrager voor de Ziektewet is moet hij deze gegevens vijf jaar bewaren. De bedrijfsarts moet de gegevens dan tien jaar bewaren.
- De bedrijfsarts mag de gegevens over de aanstellingskeuring van een medewerker maximaal zes maanden bewaren.
- De bedrijfsarts mag medische dossiers maximaal vijftien jaar bewaren.

[132] AP, *De zieke werknemer en privacy. Regels voor de verwerking van persoonsgegevens van zieke werknemers*, april 2016, p. 34 en 35

Bijlage 3. Risicomatrix

Voorschrift	Bedrijfs-onderdeel	Kans	Impact	Risico	Risicocategorie (Alternatief)	Prioriteit	Toelichting
1.							
2.							
3.							
Enz.							

Hierbij wordt een voorbeeld van een risicomatrix gegeven.

In de eerste kolom kan het voorschrift ingevuld worden. In de tweede kolom kan het bedrijfsonderdeel ingevuld worden.

- **Bij kans kan worden ingevuld hoe groot de kans is dat het voorschrift niet wordt nageleefd.**
  K = klein, M = middelgroot en G = groot.
- **Bij impact kan worden bepaald hoe groot de gevolgen zijn van niet-naleving voor de organisatie.**
  K = klein, M = middelgroot en G = groot.
- **Bij risico kan een ingeschat worden hoe groot het risico is, na analyse van kans en impact.**
  ZK = zeer klein, K = klein, M = middel, G = groot en ZG = zeer groot.
- **Bij prioriteit kan de prioriteit van de implementatie worden bepaald.**
  L = laag, M = middel en H = hoog.

Bijlage 4. Interviewvragen

Algemene vragen

1. Hoe lang bent u werkzaam in deze functie?
2. Wat houdt uw functie precies in?
3. Op welke wijze komt u in aanraking met privacy of de privacywetgeving?
4. Houdt u zich persoonlijk bezig met de verwerking van persoonsgegevens van de medewerkers?
5. Welke persoonsgegevens worden er bij op de afdeling P&O verwerkt?

Vragen m.b.t. geschreven beleid

6. Is er een privacybeleid binnen de afdeling P&O?
7. Zo ja, wat staat hier volgens u in?
8. Heeft u hier een document van? Zou u dat op kunnen sturen?

Vragen m.b.t. ongeschreven beleid

9. Is er (ook) sprake van een ongeschreven beleid? Hoe uit zich dit?
10. Zo nee, wordt er met betrekking tot privacy wel gehandeld op een bepaalde manier?

Vragen m.b.t. EPV

11. Wat weet u van wijzigingen in de privacywetgeving?
12. Wat weet u van de verplichtingen die verantwoordelijke organisaties hebben die persoonsgegevens verwerken, zoals de informatieplicht en beveiliging van die gegevens?
13. Zijn deze verplichtingen schriftelijk vastgelegd voor de afdeling P&O?
14. Worden de medewerkers waar van gegevens worden verwerkt op de afdeling P&O op de hoogte gesteld van deze verwerking?
15. Zo ja, worden zij ook op de hoogte gesteld van het doel van de verwerking
16. Worden zij ook op de hoogte gesteld van de bewaartermijn?
17. Worden medewerkers waarvan gegevens worden verwerkt gewezen op de rechten die zij hebben?
18. Zo ja, op welke manier worden de medewerkers hierop gewezen?
19. Zijn deze rechten schriftelijk vastgelegd?

Vragen m.b.t. implementatie en compliance

20. Zien de personen die met de persoonsgegevens van de medewerkers werken volgens u het belang in van privacy van die gegevens?
21. Wat vind u een goede manier om te zorgen voor bewustwording bij de medewerkers met betrekking tot het belang van het correct uitvoeren van het privacybeleid/privacy?

Bijlage 5. Uitwerkingen interviews

De uitwerkingen van de interviews zijn weggelaten in verband met de vertrouwelijkheid van deze informatie.

Bijlage 6. Privacyreglement

Reglement betreffende de bescherming van persoonsgegevens van medewerkers van het Universitair Medisch Centrum Groningen (UMCG)
september 2005

Achtergrond van het reglement

De Wet bescherming persoonsgegevens (WBP) geeft regels ter bescherming van de persoonlijke levenssfeer in verband met de verwerking van persoonsgegevens. De WBP geeft uitvoering aan artikel 10 van de Grondwet, het recht op de eerbiediging van de persoonlijke levenssfeer. Naast de verplichtingen van de WBP is voor privacyaspecten van de arbeidsrelatie van medewerkers van het UMCG ook andere wet- en regelgeving van belang. De Wet op de Ondernemingsraden (WOR) kent aan de Ondernemingsraad een instemmingsrecht toe over een privacyregeling. De Archiefwet stelt onder andere regels met betrekking tot bewaartermijnen van (persoons)gegevens in verband met de arbeidsrelatie.

De Raad van Bestuur van het UMCG onderschrijft het uitgangspunt dat zorgvuldig handelen met betrekking tot de persoonsgegevens van medewerkers van het UMCG is gewenst. Dit reglement beoogt daaraan bij te dragen. Het reglement bevat algemene regels, gebaseerd op de WBP. Privacy gegevens worden alleen aan derden verstrekt indien zij volgens dezelfde zorgvuldigheidseisen werken, zoals een gecertificeerde Arbodienst.

In verband met het verrichten van werkzaamheden en het aanwezig zijn in het UMCG zijn voor verschillende doeleinden persoonsgegevens van medewerkers noodzakelijk. De regels met betrekking tot de verzameling en verwerking van persoonsgegevens zijn voor de verschillende doeleinden niet per definitie gelijk. Zo gelden voor het in acht nemen van privacyaspecten bij ziekteverzuim en reïntegratie in de praktijk andere regels dan voor bijvoorbeeld het uitgiftesysteem van bedrijfskleding. In dit reglement wordt daarom voorzien in de mogelijkheid om per persoonsgegevensverwerking nadere (uitvoerings)regels te stellen. De Raad van Bestuur gaat er vanuit dat dit reglement en de daarop gebaseerde nadere aanvullende regels voor medewerkers en hun leidinggevenden duidelijk maakt welke rechten en plichten er bestaan inzake de persoonsgegevens van medewerkers van het UMCG.

Artikel 1 Begripsbepalingen

In dit reglement en de op basis hiervan vastgestelde nadere regelingen wordt verstaan onder:

1 UMCG: Universitair Medisch Centrum Groningen.

2 Raad van Bestuur: de Raad van Bestuur van het UMCG.

3 Verantwoordelijke: diegene die, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van de persoonsgegevens vaststelt. Inzake het UMCG is dit de Raad van Bestuur.

4 OR: Ondernemingsraad van het UMCG.

5 Functionaris voor de Gegevensbescherming (FG): de door de Raad van Bestuur benoemde functionaris die toeziet op verwerking van persoonsgegevens van zowel medewerkers als patiënten van het UMCG, overeenkomstig de WBP, het reglement en/of andere uitgevaardigde wettelijke bepalingen of regelingen dienaangaande.

6 UMCG privacy officer medewerkersgegevens: de vanuit het directoraat P&O aangewezen medewerker met uitvoerende taken, zoals omschreven in dit Privacyreglement.

7 Persoonsgegevens: elk gegeven betreffende een geïdentificeerd of identificeerbaar natuurlijk persoon.

8 Medewerker:

a. Een persoon aangesteld bij het UMCG op grond van de CAO Academische Ziekenhuizen.
b. Een persoon niet aangesteld op grond van de CAO AZ, maar die feitelijk werkzaam is bij het UMCG op grond van een:

- aanstelling bij de Rijksuniversiteit Groningen;
- detacheringovereenkomst;
- overeenkomst van het UMCG met een uitzendbureau;
- opdracht van of namens de Raad van Bestuur van het UMCG.

c. Studenten en stagiaires alsmede buitenlandse gasten en vrijwilligers die in het kader van hun opleiding, stage of studiebezoek in het UMCG activiteiten verrichten.
d. Een persoon niet meer vallend onder de categorie als bedoeld onder 1 of 2, maar van wie de gegevens nog in bestanden zijn opgenomen.

9 Betrokkene: de medewerker op wie een persoonsgegeven betrekking heeft.

10 Toestemming van de betrokkene: elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt.

11 Verwerking van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen c.q. verkrijgen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken van persoonsgegevens door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van persoonsgegevens.

12 Bestand: elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen

13 Persoonsgegevensverwerking: een middel of een samenhangend stelsel van middelen waarmee op een geautomatiseerde dan wel op een handmatige, doch systematische wijze de verwerking van persoonsgegevens plaatsvindt. Zie ook artikel 10 van dit reglement.

14 Bewerker: degene die, ten behoeve van de verantwoordelijke, persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.

15 Het College bescherming persoonsgegevens of het College: Het College dat tot taak heeft toe te zien op de verwerking van persoonsgegevens overeenkomstig het bij en krachtens de WBP bepaalde.

16 WBP: De Wet Bescherming Persoonsgegevens

Artikel 2 Reikwijdte van het reglement

1 Dit reglement is van toepassing op alle in het UMCG gehanteerde persoonsgegevensverwerkingen waarbij persoonsgegevens van medewerkers worden verwerkt.

2 In het UMCG worden in ieder geval de navolgende persoonsgegevensverwerkingen onderscheiden:

a. personeels- en salarisadministratie;

b. personeelsarchief;

c. arbo-zorgsysteem;

d. een toegangscontrole- en volgsysteem;

e. een systeem ten behoeve van de uitgifte en inname van bedrijfskleding;

f. (deels) geautomatiseerde systemen met betrekking tot werkarchieven met persoonsgegevens op (de)centraal niveau;

g. (deels) geautomatiseerde systemen voor de verwerking van persoonsgegevens in het kader van de bedrijfsvoering op decentrale werkeenheden.

3 Zowel op de hierboven genoemde persoonsgegevensverwerkingen als op eventuele toekomstige nieuwe persoonsgegevensverwerkingen zijn de bepalingen in dit reglement van toepassing, voor zover er per persoonsgegevensverwerking geen nadere regels zijn gesteld.

4 Per afzonderlijk persoonsgegevensverwerking kunnen indien noodzakelijk nadere aanvullende regels worden gesteld. Deze dienen in overeenstemming te zijn met de algemene regels zoals deze zijn omschreven in dit reglement.

Artikel 3 Algemene bepalingen

1 De Raad van Bestuur stelt het doel en de middelen voor de verwerking van persoonsgegevens vast. Voor zover dit een vaststelling, wijziging of intrekking van een regeling omtrent het verwerken of beschermen van persoonsgegevens van medewerkers betreft, is de Raad van Bestuur op grond van de Wet op de Ondernemingsraden verplicht schriftelijk om de instemming van de OR te verzoeken.

2 Onverminderd de in artikel 4 aangegeven doelstellingen (door de Raad van Bestuur met instemming van de OR vastgestelde algemene doelstellingen) worden persoonsgegevens alleen verwerkt indien aan één of meer van de volgende voorwaarden is voldaan.

Een medewerker heeft daarvoor zijn ondubbelzinnige toestemming gegeven;

Gegevensverwerking is nodig in verband met en voortvloeiend uit het dienstverband van de betrokkene;

Er is sprake van een verplichting die voortvloeit uit wet- en regelgeving, zoals bijvoorbeeld regels in het kader van de sociale wetgeving en de Wet BIG;

Indien dit noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het bestuursorgaan waaraan de gegevens worden verstrekt;

In het geval dat het gerechtvaardigde belang van de werkgever prevaleert boven het recht op bescherming van de persoonlijke levenssfeer.

3 De Raad van Bestuur is er verantwoordelijk voor dat bij de verwerking van de persoonsgegevens de volgende, door de wet daarvoor gestelde, normen in acht worden genomen:

De verwerking van de persoonsgegevens is alleen toegestaan indien dit verenigbaar is met de doeleinden waarvoor de persoonsgegevens zijn verkregen;

Er dienen maatregelen getroffen te worden die ervoor zorgdragen dat de te verwerken persoonsgegevens juist en nauwkeurig zijn. Daarbij wordt er door het UMCG naar gestreefd de persoonsgegevens zoveel mogelijk bij de medewerker zélf te verkrijgen;

De werkgever dient zodanige technische en organisatorische maatregelen te treffen dat er sprake is van een adequate beveiliging tegen verlies en onrechtmatige verkrijging van persoonsgegevens;

Bijzondere persoonsgegevens, zoals gegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid of gezondheid worden niet verwerkt, tenzij:

a. de WBP hiertoe ruimte laat;

b. de betrokkene zijn uitdrukkelijke toestemming heeft gegeven;

c. de bijzondere gegevens door de betrokkene duidelijk openbaar zijn gemaakt;

d. dit noodzakelijk is voor de vaststelling, de uitoefening of de verdediging van een recht in rechte;

e. dit noodzakelijk is ter voldoening aan een volkenrechtelijke verplichting;

f. dit noodzakelijk is met het oog op een zwaarwegend algemeen belang, passende waarborgen worden geboden ter bescherming van de persoonlijke levenssfeer en dit bij wet wordt bepaald dan wel het College bescherming persoonsgegevens ontheffing heeft verleend; in welk geval door de Raad van Bestuur nadere regels kunnen worden gesteld.

4a De Raad van Bestuur benoemt, e.e.a. conform de artikelen 62, 63 en 64 van de WBP, een functionaris, hierna te noemen de Functionaris voor de Gegevensbescherming (FG), die in het kader van de bescherming van persoonsgegevens van medewerkers toeziet op de verwerking daarvan overeenkomstig de WBP, het Reglement en/of andere uitgevaardigde wettelijke bepalingen of regelingen dienaangaande. De Raad van Bestuur kent hem daarbij de redelijkerwijs benodigde bevoegdheden toe zoals het vorderen van inlichtingen en inzage in zakelijke gegevens en bescheiden.

4b Vanuit het directoraat P&O wordt een medewerker aangesteld, hierna te noemen UMCG-privacy officer medewerkersgegevens, belast met taken, voortvloeiend uit dit Privacyreglement.

Artikel 4 Algemene doelstellingen van de persoonsgegevensverwerkingen

Bij alle verwerkingssystemen die in het UMCG worden gehanteerd waarbij persoonsgegevens van medewerkers worden verwerkt gelden één of meerdere van de volgende *algemene doelstellingen*:

a. het geven van leiding aan de werkzaamheden van medewerkers;

b. de behandeling van personeelszaken;

c. het vaststellen en doen uitbetalen van salarisaanspraken;

d. het regelen van aanspraken op uitkeringen in verband met de beëindiging van een dienstverband;

e. de opleiding en/of de ontwikkelingen van de betrokkene;

f. de bedrijfsmedische zorg voor de betrokkene;

g. het bedrijfsmaatschappelijk werk, ziektebegeleiding en casemanagement (wet Poortwachter);

h. de verkiezing van de leden van een bij wet geregeld medezeggenschapsorgaan;

i. de interne controle en de bedrijfsbeveiliging;

j. de uitvoering van een voor de betrokkene geldende arbeidsvoorwaarde;

k. het verlenen van ontslag;

l. de administratie van de personeelsvereniging, van de vereniging van oud-personeelsleden, vrijwilligers en werkgelegenheidsprojecten e.d.;

m. het innen van vorderingen, waaronder begrepen het in handen van derden stellen van die vorderingen;

n. het behandelen van geschillen en het doen uitoefenen van accountantscontrole;

o. de overgang van de betrokkene naar of diens tijdelijke tewerkstelling bij een andere afdeling van de organisatie of detachering naar een andere organisatie.

Artikel 5 Organisatie en beheer van verwerkingssystemen

1 De Raad van Bestuur neemt, overeenkomstig de eisen die de wet stelt, passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies, onrechtmatige verwerking en/of onrechtmatige inzage, resulterend in een schriftelijk document waarin per persoonsgegevensverwerking het volgende is aangegeven:

het specifieke doel van de gegevensverwerking;

- een korte beschrijving van de opzet van de persoonsgegevensverwerking;
- een beschrijving van de categorieën medewerkers en de persoonsgegevens die op hen betrekking hebben;

aan welke personen en/of instanties de persoonsgegevens eventueel verstrekt zouden kunnen worden;

een algemene beschrijving van de beveiligingsmaatregelen omtrent de persoonsgegevensverwerking en de daarbij gebruikte persoonsgegevens;

welke functionaris(sen), onverminderd de eindverantwoordelijkheid van de Raad van Bestuur, de dagelijkse verantwoordelijkheid hebben voor het technisch en organisatorisch beheer van de betreffende persoonsgegevensverwerking;

welke functionarissen bevoegd zijn om bewerkingen (het aanbrengen van mutaties in en het vernietigen van persoonsgegevens) te verrichten;

welke functionarissen toegang hebben tot (onderdelen van) de bestanden en met welk doel;

op welke wijze de toegang tot de persoonsgegevensverwerkingen voor de medewerker is geregeld en welke specifieke procedures er, mede in het kader van de bescherming van zijn rechten, zijn;

de eventuele specifieke rol en bevoegdheden van de UMCG-privacy officer medewerkersgegevens;

de eventuele nadere aanvullende regels als bedoeld in artikel 2 van dit reglement.

2 De Raad van Bestuur draagt er zorg voor dat de eventuele bij de gegevensverwerking ingeschakelde bewerker de bepalingen van de WBP alsmede de in het voorgaande lid bedoelde maatregelen en de geheimhoudingsplicht in acht neemt. Er is sprake van plichtsverzuim indien deze bepalingen niet in acht worden genomen.

3 De in lid 1 bedoelde en omschreven maatregelen worden gemeld bij de UMCG privacy officer medewerkersgegevens.

Artikel 6 Bewaartermijnen van persoonsgegevens:

1 De persoonsgegevens worden verwijderd uiterlijk twee jaren nadat het dienstverband of de werkzaamheden van de betrokkene voor UMCG zijn beëindigd, tenzij:

a. de persoonsgegevens noodzakelijk zijn ter voldoening aan een wettelijke bewaarplicht;

b. het UMCG in een specifiek geval een gerechtvaardigd belang heeft bij het langer bewaren van persoonsgegevens. In een dergelijk geval wordt betrokkene hierover schriftelijk geïnformeerd.

2 Indien de bewaartermijn is verstreken, worden de betreffende persoonsgegevens zo spoedig als redelijkerwijs mogelijk uit de persoonsgegevensverwerkingen verwijderd en vernietigd.

3 Indien de desbetreffende gegevens zodanig zijn bewerkt dat herleiding tot individuele personen redelijkerwijs onmogelijk is, kunnen zij in geanonimiseerde vorm eveneens bewaard blijven.

4 Persoonsgegevens mogen langer worden bewaard dan bepaald in het eerste lid voor zover ze voor historische, statistische of wetenschappelijke doeleinden worden bewaard, en het UMCG de nodige voorzieningen heeft getroffen ten einde te verzekeren dat de desbetreffende gegevens uitsluitend voor deze specifieke doeleinden worden gebruikt.

Artikel 7 Informatieplicht

1 De medewerker wordt op de hoogte gebracht van het bestaan van dit reglement en de eventuele daarbij behorende nadere maatregelen per persoonsgegevensverwerking, alsmede waar en op welke wijze deze zijn in te zien.

2 Een voorgenomen (deels) geautomatiseerde verwerking van persoonsgegevens voor andere doelstellingen dan genoemd in dit Reglement of eventuele nadere regels wordt, voordat met de verwerking wordt begonnen, gemeld bij de UMCG-privacy officer medewerkersgegevens. Indien genoemde verwerking op grond van artikel 27 van de Wet op de Ondernemingsraden (WOR) instemmingsplichtig is, wordt deze ter instemming voorgelegd aan de OR UMCG.

Artikel 8 Inzagerecht van medewerkers

1 Iedere medewerker heeft te allen tijde het recht zijn/haar personeelsdossier in te zien. De medewerker kan de UMCG privacy officer medewerkersgegevens verzoeken inzage te geven in de op hem betrekking hebbende persoonsgegevens en de verwerkingen die daarop plaatsvinden, mits dit geen onevenredige inspanning van de werkgever vereist. Het verzoek wordt pas ingewilligd als door de UMCG privacy officer medewerkersgegevens de identiteit van de verzoeker is vastgesteld.

2 Het verzoek om inzage wordt binnen *vier weken* afgehandeld. Ter bescherming van rechten en vrijheden van anderen kan een verzoek om inzage worden geweigerd. Een weigering wordt altijd schriftelijk met redenen omkleed.

3 Per persoonsgegevensverwerking kan, met inachtneming van de leden 1 en 2 van dit artikel de procedure met betrekking tot het indienen en afhandelen van een verzoek nader worden geregeld.

Artikel 9 Recht op correctie of afscherming van persoonsgegevens

1 Iedere medewerker heeft het recht om de privacy officer medewerkersgegevens te verzoeken om hem betreffende persoonsgegevens te corrigeren (aan te vullen, te verbeteren of te verwijderen) of af te schermen indien:

deze gegevens feitelijk onjuist zijn; en/of

deze gegevens voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn; en/of

anderszins in strijd zijn met een wettelijk voorschrift, dit reglement of hierop gebaseerde nadere regelingen per persoonsgegevensverwerking.

2 De medewerker geeft in zijn verzoek aan welke wijzigingen aangebracht moeten worden.

3 Het UMCG draagt zorg voor een deugdelijke vaststelling van de identiteit van de verzoeker door middel van officiële legitimatie.

4 Het is niet mogelijk om correcties aan te brengen als daarmee de belangen van anderen, waaronder de werkgever, aangetast worden. In dat geval zal het schriftelijke verzoek om

correctie aan het personeelsdossier worden toegevoegd. Het schriftelijke verzoek om correctie zal eveneens aan het personeelsdossier worden toegevoegd, als het aanbrengen van correcties om technische redenen niet mogelijk is.

5 De UMCG privacy officer medewerkersgegevens neemt binnen *vier weken* een beslissing op het verzoek. Zonodig wordt de medewerker in de gelegenheid gesteld een nadere toelichting te geven. De UMCG privacy officer medewerkersgegevens kan beslissen het verzoek als bedoeld in lid 1 weigeren. Een weigering van het verzoek wordt schriftelijk met redenen omkleed. Het verzoek om correctie wordt, tezamen met deze weigering, opgeborgen in het dossier van de medewerker.

6 De Raad van Bestuur draagt er zorg voor dat een beslissing tot wijziging of afscherming van persoonsgegevens zo spoedig als redelijkerwijs mogelijk wordt uitgevoerd.

7 Per persoonsgegevensverwerking kan, met inachtneming van de bovenstaande bepalingen, de procedure met betrekking tot het indienen en afhandelen van een verzoek tot wijziging of afscherming van persoonsgegevens nader worden geregeld.

Artikel 10 Rechtsbescherming

1 Als een medewerker het niet eens is met een beslissing op een verzoek tot inzage, een beslissing tot (gedeeltelijke) afwijzing van het verzoek tot correctie, afscherming, verbetering of aanvulling van persoonsgegevens of een beslissing naar aanleiding van een aantekening van verzet kan deze een bezwaarschrift indienen bij de Raad van Bestuur. De Regeling Rechtspositionele Besluiten is van overeenkomstige toepassing.

2 Binnen 6 weken na ontvangst van de beslissing van de Raad van Bestuur omtrent het bepaalde in lid 1 van dit artikel, moet het verzoekschrift om herziening van de beslissing worden ingediend. De medewerker kan zich hiermee wenden tot de bestuursrechter.

3 De medewerker kan zich, binnen de beroepstermijnen zoals die gelden voor een beroep op grond van de AWB, tevens wenden tot het College bescherming persoonsgegevens met het verzoek om bemiddeling of advies inzake zijn geschil met de Raad van Bestuur.

Artikel 11 Slot- en overgangsbepalingen

Dit reglement is vastgesteld na instemming van de OR. Wijzigingen in het reglement kunnen slechts worden doorgevoerd met inachtneming van de instemming van de OR.

Regels ter nadere uitwerking van dit reglement, zoals bedoeld in artikel 2, worden door de Raad van Bestuur vastgesteld.

Dit reglement is ingegaan op 1 februari 2003 en is gewijzigd in september 2005 (besluit 182.560/RvB 8 december 2004).

Bijlage 7. UMCG-gedragscode

INLEIDING

Onze missie “Bouwen aan de toekomst van gezondheid” maken wij waar met competente medewerkers die integer handelen. Het UMCG heeft een publieke functie. De samenleving merkt en ziet veel van wat wij doen. Wij werken als het ware in een glazen huis, maximale transparantie is dus nodig. Als wij openheid, respect en eerlijkheid naar onze klanten (te weten patiënten en hun familie, maar ook andere externe relaties, zoals leveranciers) willen uitstralen, zullen wij intern ook zo moeten handelen. Juist omdat wij vooral dan een extra dimensie kunnen geven aan ons professionele handelen.

Deze integriteitscode geeft aan wat wij in het UMCG verstaan onder integriteit en waar onze grenzen liggen. In de omgang met onze klanten en met elkaar gebruiken wij de volgende waarden:

- Respectvol

Respectvol omgaan met elkaar betekent de ander in zijn waarde laten en respect opbrengen voor iemands opvattingen of rechten, of voor materiële zaken zoals andermans eigendom.

- Betrouwbaar

Betrouwbaar betekent open en eerlijk zijn naar patiënten (en hun familie), andere externe relaties en collega’s. Collega’s en leidinggevenden aanspreken op slecht gedrag en complimenteren bij goed gedrag, maar ook afspraken (op correcte wijze) nakomen.

- Betrokken

Medewerkers zijn betrokken bij hun werk. Dit betekent het nemen van verantwoordelijkheid, indien dat nodig is ook buiten de eigen werksituatie. En blijvende motivatie voor ontwikkeling in en buiten het eigen vakgebied.

- Veilig

Patiënten, bezoekers en medewerkers moeten zich in het UMCG veilig voelen. Daar hoort ook bij veilig werken, volgens bestaande richtlijnen en protocollen.

Deze waarden vormen de basis voor het dagelijks handelen van alle UMCG’ers. Het is soms moeilijk om vast te stellen wat dat nu betekent voor de dagelijkse praktijk. Op vragen als ‘mag ik een fles wijn aannemen van een zakelijke relatie’ of ‘mag ik een mailtje sturen van mijn werk-pc naar mijn reisbureau’ geven bovengenoemde waarden geen direct antwoord. Heldere richtlijnen kunnen houvast bieden. De afgelopen jaren zijn er op diverse onderwerpen nadere regels geformuleerd hoe te handelen in verschillende situaties. Soms liggen ze vast in de CAO UMC en soms in eigen UMCG-regelingen.
Voortbouwend op bestaande richtlijnen biedt deze integriteitscode een plek waarin de meeste integriteitsvraagstukken beschreven worden. Het eerste deel van de code bestaat uit bundeling en verwijzing naar de al bestaande regels binnen het UMCG. In het tweede deel wordt op een aantal punten nieuwe richtlijnen geformuleerd.

Daarnaast blijven er altijd situaties waarvoor geen regels bestaan of waarin niet direct duidelijk is hoe je daarin moeten handelen. Daarvoor vallen wij dan terug op onze waarden. Ze hebben zowel betrekking op het handelen van de medewerker in contact met patiënten en hun naasten en andere externe relaties, als op de onderlinge verhoudingen.

Samengevat: bij alles wat wij doen in het UMCG handelen wij respectvol, betrouwbaar, betrokken en veilig.

Tenslotte wordt op het eind van deze code ingegaan op de rol van de leidinggevende en de mogelijke sancties op het overtreden van regels en normen.

BESTAANDE UMCG-REGELINGEN OP HET GEBIED VAN INTEGRITEIT

De afgelopen jaren zijn binnen het UMCG al diverse regelingen op het terrein van integriteit ontwikkeld. Hierna volgt een overzicht van de verschillende regelingen met een korte toelichting.

1. Omgangsvormen

Klachtenregeling medewerkers UMCG (*/198.047)
Klachtenregeling voor patiënten en bezoekers (Klachtenreglement UMCG 1998)
Rookbeleid UMCG (juli 2004, 179.437/RvB)
Kledingrichtlijnen voor het UMCG (mei 1998)

Wij gaan in ons werk op een respectvolle manier om met de patiënt, zijn naaste, en met de eigen collega's. Dit betekent dat wij de ander serieus nemen en een respectvolle houding hebben voor andere standpunten, visies en inbreng van anderen. De respectvolle houding komt onder andere tot uiting in collegialiteit, teamgeest, openheid en klantgerichtheid.

Een ander onderdeel is het respect tonen voor de individuele verscheidenheid en het nastreven van correcte omgangsvormen. Dit betekent dat medewerkers hun werkzaamheden verrichten zonder daarbij onderscheid te maken op grond van godsdienst, levensovertuiging, politieke gezindheid, ras, geslacht of andere persoonsgebonden kenmerken. Beledigingen, discriminatie, seksuele intimidatie en pesten zijn uitingen van ongewenste omgangsvormen, we laten hiermee immers geen respect voor de ander zien.

Verder houdt respectvol omgaan met anderen bijvoorbeeld ook in dat de medewerker de regels over (niet) roken in acht neemt. Zowel ten opzichte van de collega's, als ten opzichte van de patiënt en de bezoeker. Ook draagt de medewerker zijn UMCG-pas zichtbaar op de kleding, zodat hij herkenbaar is als UMCG-medewerker. Ook ziet hij er verzorgd uit; de kleding past bij de uitoefening van de functie.

2. Vertrouwelijke informatie en omgang met media

Wet Bescherming Persoonsgegevens (WBP), Privacyreglement UMCG
Wet op de Geneeskundige Behandelovereenkomst (WGBO)
Artikel 9.8 CAO UMC
Professioneel Statuut voor medische specialisten (bijlage I, CAO UMC)
Instructie arts-assistenten UMCG (*/74.193, januari 1996)

Soms beschikt de medewerker ook over gegevens of informatie, waarvan hij kan begrijpen dat deze informatie in handen van anderen - collega's of buitenstaanders - de belangen van de patiënt of medewerker of het UMCG kunnen schaden. De medewerker mag vertrouwelijke informatie dan ook niet met collega's of anderen bespreken, tenzij dit een functioneel karakter heeft, dat wil zeggen: voor het werk noodzakelijk is.

Veel medewerkers van het UMCG hebben toegang tot persoonlijke gegevens van patiënten en/of van anderen. Denk aan informatie over de aard van de ziekte van een patiënt of het doorgeven van

adresgegevens van een medewerker aan een derde. De regel is dat gegevens van patiënten of anderen niet openbaar gemaakt mogen worden, als deze daardoor tot op de persoon herleidbaar zijn. Dat wil zeggen: nóch schriftelijk nóch mondeling, nóch via andere communicatiemiddelen, zoals Internet.

Een uitzondering geldt voor die situaties waarin wij op basis van wet- of regelgeving gehouden zijn persoonlijke gegevens te verstrekken. Bij twijfel wordt met de leidinggevende afgestemd. Meer in het bijzonder geldt voor de beroepen zoals verpleegkundigen en artsen het medische beroepsgeheim. In verband met patiëntgegevens zijn ook van belang: De Wet op de Geneeskundige Behandelovereenkomst (WGBO), het Professioneel Statuut voor Medisch Specialisten en de Instructie arts-assistenten (al dan niet in opleiding) UMCG.

Werkplek
De medewerker draagt er zorg voor dat bij het verlaten van de werkplek deze zo goed mogelijk is opgeruimd, zodat vertrouwelijke informatie voor derden niet toegankelijk is. Ook de computer is uit of zodanig beveiligd dat een derde daar geen toegang toe heeft.

Media
Mondelinge en schriftelijke informatie wordt alleen aan de media wordt gegeven als dat overlegd is met de persvoorlichter of Hoofd Communicatie.

3. E-mail, intranet, Internet en andere bedrijfsmiddelen

Wetboek van Strafrecht, o.a. de artikelen 137c tot en met 137g
Gedragscode internet- en e-mail gebruik (januari 2004)
Beleid alcohol, medicijnen en drugs (oktober 1998)

E-mail en internet
Tijdens het werk kan de medewerker gebruik maken van e-mail en intranet en het Internet bezoeken. Deze worden aan de medewerker beschikbaar gesteld en zijn in beginsel alleen bedoeld om efficiënt en effectief voor het werk in te zetten. Gebruik ervan is dus verbonden aan taken die voortvloeien uit de functie.

Onder strikte voorwaarden is zeer beperkt privé-gebruik van e-mail en Internet toegestaan. Voorwaarden zijn dat het gebruik niet storend is voor de dagelijkse werkzaamheden of de functievervulling schaadt en voorts geen verboden gebruik oplevert. Zo is het de medewerker bijvoorbeeld niet toegestaan via de internetfaciliteiten van het UMCG sites te bezoeken die pornografisch, racistisch, discriminerend, aanstootgevend of beledigend materiaal bevatten.

Voor Internet- en e-mailgebruik is een gedragscode opgesteld, die sinds 1 februari 2004 van toepassing is. Daarin zijn ook regels opgenomen voor (steekproefsgewijze) controles door ICT.

Andere bedrijfsmiddelen
Los van e-mail en Internet zijn er ook andere bedrijfsmiddelen die de medewerker tot zijn beschikking heeft, zoals pen/papier, printer/kopieerapparaat, telefoon. Ook hiervoor geldt dat deze middelen in beginsel alléén bedoeld zijn om te gebruiken voor het werk.

Een enkel kopietje maken voor privé-gebruik of in werktijd een kort privé-telefoongesprek zal echter in de meeste gevallen niet als ongeoorloofd of overmatig gebruik van de bedrijfsmiddelen worden aangemerkt.

De medewerker gaat zorgvuldig om met de bedrijfsmiddelen die hem of haar ter beschikking worden gesteld. Meer in het bijzonder gelden ten aanzien van bedrijfskleding aparte richtlijnen, zoals ten aanzien van de hygiëne (waar kleding wel of niet gedragen mag worden). Meer informatie is te vinden in de Kledingrichtlijnen UMCG, het Handboek P&O en de website van de Facilitaire Dienst.

Medicijnen / Medische hulpmiddelen
Binnen het UMCG hebben sommige medewerkers vanwege hun functie toegang tot de voorraad medicijnen/verdovende middelen en medische hulpmiddelen, maar ook b.v. voedingsmiddelen bestemd voor patiënten. Deze bedrijfsmiddelen zijn alleen voor patiënten en mogen niet gebruikt worden voor eigen gebruik van de medewerker.

4. Nevenwerkzaamheden Artikel
9.3. CAO UMC
Handboek Personeel & Organisatie

Veel medewerkers van het UMCG zijn - betaald of onbetaald - in hun vrije tijd actief bijvoorbeeld als bestuurslid, docent of als auteur. In die gevallen waarin de nevenwerkzaamheden een relatie hebben met de functie van de medewerker dan wel de werkgebieden van het UMCG, is hiervoor toestemming vereist. Voor activiteiten in de privé-sfeer (sport, politiek) geldt dat dus in beginsel niet, tenzij dit consequenties heeft voor het werk. Dit kan het geval zijn als de activiteiten een zodanige omvang hebben dat daardoor de concentratie en productiviteit van de medewerker nadelig wordt beïnvloed.

Het is in eerste instantie de medewerker zélf, die beoordeelt of toestemming vereist is. Bij twijfel wordt de medewerker geadviseerd hierover contact op te nemen met de leidinggevende.

Als handvat voor die beoordeling (voor zowel medewerker als leidinggevende) gelden de volgende punten:

- Karakter van de nevenwerkzaamheden.
- Functie van de medewerker in de organisatie.
- Het gebied waarin de nevenwerkzaamheden worden verricht.
- Verwevenheid met de (hoofd)functie in het UMCG.
- Komt de betrouwbaarheid en integriteit van de medewerker in het geding.
- Bestaat het risico dat de ambtelijke informatie bij de uitoefening van de nevenwerkzaamheden wordt misbruikt.
- De reputatie van het bedrijf of de branche waarin de nevenwerkzaamheden worden verricht.
- Is er een risico dat de medewerker in een (oneigenlijke) afhankelijkheidspositie terecht komt c.q. is er een risico dat daardoor een goede en onafhankelijke uitoefening van de werkzaamheden in het ziekenhuis in het geding komt.

In het handboek P&O is de werking van artikel 9.3 CAO UMC nader toegelicht en is ook een formulier beschikbaar voor het verkrijgen van toestemming.

Inkomsten onder de € 2.200, - per jaar mag een medewerker behouden. Over inkomsten die boven dit bedrag uitkomen en waarvoor geldt dat de nevenwerkzaamheden in het verlengde liggen van de functie van de medewerker, moeten nadere afspraken worden gemaakt.

5. Wetenschappelijk onderzoek

Wet Medisch-wetenschappelijk Onderzoek met mensen (WMO)
Reasearchcode UMCG, juli 2007

Naast patiëntenzorg en onderwijs is het verrichten van (medisch)wetenschappelijk onderzoek een van onze kerntaken. Van belang is dat dit onderzoek op een zorgvuldige en integere wijze plaatsvindt. De uitgangspunten en te hanteren richtlijnen bij het verrichten van (medisch) wetenschappelijk onderzoek zijn vastgelegd in een aparte researchcode UMCG. De medewerker houdt in het kader van

wetenschappelijk onderzoek rekening met de vertrouwelijkheid van gegevens gedurende het hele proces van onderzoek.

6. Klokkenluiders

Klokkenluidersregeling, nog vast te stellen (2008)

Tekst wordt na vaststelling klokkenluidersregeling aangevuld.

AANVULLENDE RICHTLIJNEN OP HET TERREIN VAN INTEGRITEIT

Op een aantal onderwerpen zoals het aanvaarden van geschenken en uitnodigingen bestaat er tot dusverre binnen het UMCG geen expliciete richtlijnen.

1. Geschenken

Geschenken of giften mogen nooit worden aangenomen in ruil voor een tegenprestatie. In zakelijke relaties komt het geregeld voor dat iets aan de ander wordt aangeboden, zonder dat daar direct een tegenprestatie tegenover staat. Daaraan kunnen evenzeer integriteitsrisico's verbonden zijn. Het is dan ook om deze reden dat we met het aannemen van geschenken en andere voordelen uiterst terughoudend moeten omgaan.

De volgende richtlijnen/criteria zijn van toepassing bij het aannemen van geschenken/voordelen:

- Geschenken of een dienst met een (geschatte) waarde van € 50, - of meer worden niet geaccepteerd, dan wel geretourneerd naar de gever. Bij twijfel vindt overleg plaats met de leidinggevende.
- Geldbedragen worden nooit geaccepteerd.
- Geschenken van derden die verband houden met het werk zijn in principe eigendom van het UMCG. Geaccepteerde geschenken worden dan ook gemeld aan de leidinggevende.
- Aanbiedingen aan de medewerker persoonlijk voor korting op privé-goederen worden niet geaccepteerd
- Bedrijfsattenties die breed en routinematig worden verspreid, zoals agenda's, kalenders, pennen, muismatten of andere hebbedingetjes mogen worden geaccepteerd/hoeven niet te worden gemeld, tenzij deze de waarde van € 50,- overstijgen.

2. Uitnodigingen voor reizen, congressen, diners en evenementen

Medewerkers hebben op dit punt een eigen verantwoordelijkheid en moeten voorkomen dat door aanvaarding van een dergelijke uitnodiging er een afhankelijkheidsrelatie ontstaat ten opzichte van de derde. Bij twijfel is het van belang om vooraf overleg te hebben met de leidinggevende.

Verder wordt van de medewerker verwacht dat hij bij informele contacten met derden, zoals etentjes en recepties waar alcohol wordt geschonken, zijn verantwoordelijkheid neemt. Hij loopt immers ook dan rond als representant van het UMCG.

3. Werkzaamheden die inkomsten/subsidies genereren

Voorzover medewerkers uit hoofde van hun functie bij het UMCG financiën of subsidies verwerven, komen deze ten goede van het UMCG c.q. worden deze gestort op de rekening van het UMCG, tenzij hierover met de Raad van Bestuur of de voorzitter sectordirectie de afspraak wordt gemaakt dat dit op een aparte Stichtingenrekening moet worden geboekt. In dat geval worden duidelijke afspraken gemaakt over de wijze waarop deze middelen worden aangewend.

Als regel geldt dat eventuele (on)kostenvergoedingen aan UMCG-medewerkers worden uitgekeerd conform de regels van de CAO of andere UMCG-regelgeving en dat aan een medewerker totaal nooit meer vergoed kan worden dan waarop hij of zij krachtens de CAO recht zou hebben.

HANDHAVINGSBELEID

In de eerste plaats heeft iedere medewerker een eigen verantwoordelijkheid om zich aan de hiervoor geformuleerde regels en normen te houden en zonodig anderen hierop aan te spreken. Onderdeel van integer handelen is verder dat de medewerker dubieuze zaken, zoals vermoeden van fraude, corruptie, diefstal, in beginsel altijd direct aan de leidinggevende meldt.

Daarnaast heeft de leidinggevende een bijzondere verantwoordelijkheid en voorbeeldfunctie. Tenslotte kan de werkgever bij (ernstige) overtredingen van de regels en normen overgaan tot het opleggen van sancties.

1. Rol van leidinggevende

De leidinggevende geeft het goede voorbeeld, ook als het gaat om de vraag hoe om te gaan met integriteitsvraagstukken. Van de leidinggevende wordt verwacht dat hij zonodig integriteitsvraagstukken bespreekbaar maakt, bijvoorbeeld in werkoverleggen. Een open houding daarin stimuleert medewerkers hetzelfde te doen. De leidinggevende moet ook zelf aanspreekbaar zijn op zijn handelen/uitlatingen, die door anderen als niet integer worden beschouwd. De leidinggevende onderzoekt meldingen inzake schending van de integriteitsregels en treft zonodig nadere maatregelen.

2. Overtreden van regels en normen

Hoofdstuk 10 en 11 CAO UMC

Bij overtreding van regels en normen (ook die niet in deze Integriteitscode staan, zoals regels bij ziek- en herstelmelding en werktijdafspraken) is in beginsel sprake van een situatie dat de medewerker zich niet gedraagt zoals van hem verwacht wordt. Hiervoor kan een medewerker disciplinair wordt gestraft. Hij heeft zich dan schuldig gemaakt aan plichtsverzuim. Ook in de privé-sfeer kan een

medewerker zich schuldig maken aan plichtsverzuim. Het gaat dan wel om gedrag dat de belangen van het UMCG schaadt of waardoor twijfel rijst over de integriteit als medewerker van het UMCG. Denk aan een voorbeeld van een beroepsbeoefenaar die betrokken is bij illegale zorgpraktijken.

In bijzondere gevallen kan overtreding van bepaalde regels bovendien aanleiding zijn voor een op non-actief stelling. Dit is een tijdelijke (orde-)maatregel. Dit gebeurt in situaties waarin continuering van de werkzaamheden tijdelijk niet langer verantwoord is. Zo kan ingeval van diefstal kan de vertrouwenskwestie heel sterk spelen. Disciplinaire straffen variëren van schriftelijke berisping als lichtste straf tot strafontslag als zwaarste straf. Welke straf wordt opgelegd hangt af van de ernst van het plichtsverzuim. Veel hangt ook af van de omstandigheden waaronder het plichtsverzuim zich heeft voorgedaan of de mate waarin dat verzuim de medewerker kan worden aangerekend.
De CAO UMC kent voorts nog een aantal andere sancties voor overtreden regels. Hierbij gaat het bijvoorbeeld om ziektevoorschriften e.d. In voorkomende gevallen zullen deze regels worden toegepast.

TOT SLOT

Voordat deze integriteitscode uitkwam hadden wij in het UMCG natuurlijk ook al normen, waarden en regels. Sommige impliciet, sommige al neergelegd in een regeling. Zo komt duidelijk tot uiting in de klachtenregeling voor medewerkers dat wij respectvol met elkaar omgaan. De meeste medewerkers van het UMCG hielden zich uit zich zelf al aan de waarden, daarvoor is deze integriteitscode niet nodig. Toch hebben wij ons beleid vastgelegd, als een handvat voor iedereen. Bij twijfel kunnen wij er op terugvallen. En de buitenwereld weet waar wij voor staan.

Bijlage 8. Gedragscode UMCG Internet- en emailgebruik

Algemeen

Inleiding

Medewerkers van het UMCG beschikken veelal over internet- en e-mailfaciliteiten voor de uitvoering van de werkzaamheden. Deze gedragscode geeft aan op welke wijze medewerkers in het UMCG behoren om te gaan met internet en e-mail. Naast regels voor het gebruik worden de verschillende risico's van internet en e-mail benoemd. Tevens wordt aangegeven op welke wijze de controle op naleving van deze gedragscode plaatsvindt. De leiding van een organisatieonderdeel van het UMCG kan - passend binnen deze gedragscode - nadere aanwijzingen geven met betrekking tot het gebruik van internet en e-mail.

Bij de totstandkoming van deze gedragscode is het Privacyreglement UMCG in acht genomen.

Doelstellingen

Met de gedragscode beoogt het UMCG:

- aan medewerkers en management duidelijk te maken dat de bedrijfsmiddelen internet en e-mail in beginsel alleen bedoeld zijn als efficiënte hulpmiddelen bij het werk;
- duidelijkheid te geven over de aard en wijze waarop gebruik mag worden gemaakt van de internet- en e-mailfaciliteiten;
- de bewustwording te vergroten van het gebruik van internet en e-mail en de daaraan verbonden risico's;
- negatieve gevolgen, zoals het binnenhalen van virussen of ongewenste publiciteit, voor het UMCG te voorkomen.

Werkingssfeer

Deze gedragscode is van toepassing op iedere medewerker[133] van het UMCG en een ieder die hieraan is gelijk gesteld op grond van het Privacyreglement UMCG.

Risico's

Gebruik maken van internet- en e-mailfaciliteiten is voor velen in het UMCG nodig om het werk goed te doen. Echter, onjuist en onnodig gebruik kost het UMCG geld, tijd en capaciteit van mensen en apparatuur en brengt diverse risico's met zich mee. Zo kan door het downloaden van grote bestanden de ICT-infrastructuur van het UMCG te hoog worden belast. Ook kunnen bij het ontvangen van mail virussen binnengehaald worden. Door het gebruik van internet en e-mail voor niet-werkgerelateerde doeleinden worden onnodig kosten gemaakt op rekening van het UMCG. Medewerkers dienen zich hiervan bewust te zijn. Tegen de achtergrond van de risico's van het gebruik van internet en e-mail en het niet-werkgerelateerde gebruik wordt van de werknemers professioneel en integer handelen verwacht.

Regels voor het gebruik

[133] Voor de definitie van het begrip medewerker wordt verwezen naar artikel 1 lid 7 Privacyreglement UMCG. Het betreft iedereen die werkzaamheden voor het UMCG verricht en daarbij kan beschikken over internet- en e-mailfaciliteiten. Dat wil zeggen dat deze gedragscode ook van toepassing is op o.a. RUG-medewerkers, gedetacheerden, uitzendkrachten, studenten, stagiairs, vrijwilligers, gasten e.d. op het moment dat zij gebruik maken van de internet- en e-mail faciliteiten van het UMCG.

1. Het gebruik van internetfaciliteiten en e-mailfaciliteiten door medewerkers van het UMCG houdt verband met taken die voortvloeien uit de functie en heeft in beginsel een zakelijk karakter. Alle handelingen die in strijd zijn met de belangen van het UMCG zijn verboden.

2. In de combinatie en samenloop van werk- en privétijd is het gebruik van deze faciliteiten voor privé- doeleinden in zeer beperkte mate toegestaan. In dat geval houdt de medewerker zich aan de volgende punten:

    a. De medewerker gaat op een verantwoorde wijze om met het privé-gebruik en zorgt er voor dat het onder geen beding storend is voor de dagelijkse werkzaamheden.

    b. Wanneer de medewerker voor privé-doeleinden gebruik maakt van de e-mail faciliteit van het UMCG moet duidelijk zijn dat het UMCG op geen enkele wijze gebonden is dan wel hiermee in verband staat.

    c. Tevens houdt hij zich hierbij aan alle in deze gedragscode gestelde regels.

3. Het volledig veilig verzenden van e-mail berichten is nog steeds niet gegarandeerd. Medewerkers worden geacht hier met alle mogelijke voorzichtigheid mee om te gaan en in ieder geval de volgende zaken in acht te nemen:

    a. De medewerker is persoonlijk verantwoordelijk voor het gebruik van de aan hem toegekende rechten voor systemen en middelen.

    b. Patiëntgerelateerde informatie die direct tot de persoon herleidbaar is mag alleen dan per e mail vanuit het UMCG naar buiten worden verstuurd als de verzender zich ervan vergewist heeft dat de ontvanger de privacy van de patiënt zal borgen. Het UMCG heeft hiertoe tevens een passage opgenomen in de disclaimer bij externe e-mail berichten.

    c. Bedrijfsgevoelige informatie mag niet per e-mail vanuit het UMCG naar buiten worden verstuurd, tenzij de Raad van Bestuur hiervoor toestemming heeft verleend.

    d. De medewerker stelt niet aan derden (gedeelten van) het interne UMCG adresboek met e-mail adressen beschikbaar.

4. Het is niet toegestaan om via de internetfaciliteiten van het UMCG:

    a. Sites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten. Hieronder vallen ook erotisch getinte sites en dating sites. Ook het bezoeken van sites die bestemd zijn om te gokken danwel het bezoeken van chat- /babbelboxen is niet toegestaan.

    b. Sites te bezoeken die met name bedoeld zijn voor ontspanning en vermaak door het aanbieden van spelletjes, puzzels, muziek etc.

    c. Zich ongeoorloofd toegang te verschaffen tot niet openbare bronnen op internet.

    d. Materiaal te downloaden. Deze mogelijkheid is centraal zo veel mogelijk geblokkeerd. Indien het downloaden van materiaal voor de functie noodzakelijk is, dan kan bij de helpdesk ICT informatie verkregen worden hoe hier ontheffing voor kan worden verkregen.

5. Het is niet toegestaan om via de e-mailfaciliteiten van het UMCG:

    a. Formele correspondentie te voeren. Formele correspondentie wordt uitsluitend schriftelijk gevoerd en volgens de daarvoor bestaande instructie geregistreerd en gearchiveerd.

    b. Berichten anoniem of onder een fictieve naam te versturen.

    c. Berichten te versturen die een inhoud of bijlagen hebben zoals onder 3c en 3d vermeld.

    d. Ketting-mailberichten te verzenden of door te sturen.

e. Ten behoeve van privé-gebruik abonnementen te nemen op nieuwsbrieven c.q. deel te nemen aan nieuwsgroepen.

f. Iemand lastig te vallen door middel van onnodige en/of ongewenste berichten.

Maatregelen aan het UMCG Area Network (AAN)

6. De afdeling ICT treft in opdracht van de Raad van Bestuur in het kader van deze gedragscode een aantal technische maatregelen met betrekking tot de internet- en e-mailfaciliteiten. Dit betreft o.a. de volgende maatregelen:

   a. Het zoveel mogelijk centraal blokkeren van internetsites (ook de chatfunctie) zoals bedoeld onder 4a en 4b van deze gedragscode.

   b. Binnenkomend en uitgaand internet en e-mailverkeer wordt gecontroleerd op virussen e.d. Als een e-mailbericht een virus bevat, dan wordt dit in principe automatisch tegengehouden. De ontvanger wordt hierover geïnformeerd De inhoud wordt doorgestuurd maar kan mogelijk verminkt zijn. Mocht ondanks deze centraal genomen maatregel, een gebruiker het vermoeden hebben dat een virus is binnengekomen, dan meldt hij dit aan de helpdesk van ICT.

   c. Het zoveel mogelijk tegen gaan van inbraakpogingen van binnenuit en buitenaf.

Controle

7. Om de veiligheid van het netwerk te waarborgen en toe te zien op een zorgvuldig gebruik overeenkomstig deze gedragscode worden van tijd tot tijd steekproefsgewijs controles uitgevoerd door daartoe aangewezen medewerkers van de ICT, onder verantwoordelijkheid van het Hoofd ICT-Beheer, naar de tijdsbesteding, bezochte sites en e-mail-verkeer. Bij deze vorm van controle wordt niet naar de inhoud van het berichtenverkeer gekeken. Intranetgebruik wordt niet gecontroleerd. ICT rapporteert bijzonderheden in het gebruik van de internet- en e-mailfaciliteiten aan de desbetreffende afdelingsleiding.

~~8.~~ Controle door de daartoe aangewezen medewerkers van de ICT op de aard en inhoud van het gebruik vindt in zijn algemeenheid slechts plaats indien daartoe naar het oordeel van de afdelingsleiding aanleiding bestaat. Deze aanleiding kan o.a. bestaan uit klachten, signalen van binnen of buiten het UMCG en systeemstoringen. In dat geval kan de afdelingsleiding ICT verzoeken de gegevens van de betreffende gebruiker te openen en te bekijken. Hieronder valt mede het openen van e-mail, ook die voor privé-gebruik.

9. Indien onderzoek zoals vermeld onder punt 8 op verzoek van de betreffende afdelingsleiding plaatsvindt inzake de inhoud van internet- en/of e-mail gebruik, zal de betreffende medewerker daarvan vooraf op de hoogte worden gebracht.

10. De informatie verkregen uit de controles wordt bewaard zolang dit nodig is voor nader onderzoek en eventueel te treffen maatregelen. Daarna vindt binnen drie maanden vernietiging van de informatie plaats.

11. De ICT treft in opdracht van de Raad van Bestuur zodanige maatregelen dat de controles zoals vermeld in deze gedragscode in alle zorgvuldigheid en met alle noodzakelijke waarborgen voor de privacy van de gebruiker(s) worden uitgevoerd.

Sancties

12. Overtreding van deze gedragscode kan gevolgen hebben voor de rechtspositie van de betreffende medewerker. Afhankelijk van de aard van de overtreding kan een disciplinaire maatregel worden getroffen. De Regeling Rechtspositionele Besluiten UMCG is hierbij van toepassing.

Slot

13. In alle gevallen waarin deze gedragscode niet voorziet, beslist de Raad van Bestuur.

14. Deze gedragscode is vastgesteld door de Raad van Bestuur met instemming van de Ondernemingsraad en treedt in werking per 1 februari 2004.

    Wijzigingen op deze gedragscode behoeven de instemming van de Ondernemingsraad.