Contractbeheer als privacy instrument

Niels Keller

UMC-staf Juridische Zaken
Hanzehogeschool Groningen
Instituut voor Rechtenstudies

Groningen, juni 2015

Studentenbureau UMCG

Universitair Medisch Centrum Groningen

Contractbeheer als privacy instrument

Een onderzoek naar de wijze waarop er binnen de sectoren/ afdelingen van het UMCG het contractbeheer (opnieuw) kan worden ingericht, met de Europese Privacy Verordening als uitgangspunt en rekening houdend met de verschillende belangen van de sectoren/ afdelingen binnen het UMCG.

Groningen, juni 2015

Auteur	Niels Keller
Studentnummer	290873
Afstudeerscriptie in het kader van	Europese Privacy Verordening, contractbeheer HBO-Rechten Hanzehogeschool Groningen
Opdrachtgever	Mr. Robert Jager UMC-staf|Juridische Zaken, UMCG
Begeleider onderwijsinstelling	Dr. Michael Riemens HBO-Rechten Hanzehogeschool Groningen
Begeleider UMCG	B.M.Y. Sieperda UMC-staf|Juridische Zaken, UMCG

Trefwoorden: Europese Privacy Verordening, Compliance, Contractbeheer

Voorwoord

Voor u ligt het eindresultaat van mijn opleiding HBO-Rechten. Tijdens de opleiding HBO-Rechten heb ik veel kennis mogen opdoen over allerlei rechtsgebieden. In dit onderzoek heb ik kennis opgedaan over een voor mij nieuw onderwerp in het kader van de Europese Privacy Verordening en het contractbeheer.

Graag wil ik de personen bedanken die hebben bijgedragen aan de totstandkoming van mijn afstudeeronderzoek. Allereerst mijn opdrachtgever Robert Jager, zonder wie ik dit onderzoek niet had kunnen uitvoeren. Daarbij wil ik Cathy Zelhorst bedanken. Dan wil ik graag mijn praktijkbegeleidster Boudien Sieperda bedanken, gezien zij mij tijdens de afstudeerperiode voorzien heeft van goede tips en advies. Daarnaast wil ik iedereen bedanken uit het team van de Privacy-werkorganisatie. De periode binnen het team heb ik als zeer prettig ervaren. Tevens wil ik iedereen bedanken die heeft meegewerkt aan de interviews en daarnaast de medewerkers van het Universitair Medisch Centrum Groningen, waar ik gesprekken mee heb gevoerd. Zonder deze mensen had ik geen praktijkonderzoek kunnen verrichten.

Verder wil ik mijn afstudeerdocent Michael Riemens bedanken voor zijn begeleiding gedurende het afstudeerproces. De laatste personen die ik wil bedanken, zijn mijn ouders, Kor Keller en Jegien Keller-Dijkstra. Zij hebben mij ten eerste de kans gegeven om HBO-Rechten te studeren en daarnaast hebben zij mij gedurende de opleiding altijd voorzien van goed advies en steun.

Dan wens ik u tenslotte veel leesplezier toe!

Niels Keller

Groningen, juni 2015

INHOUDSOPGAVE

SAMENVATTING

De aanleiding van dit onderzoek is een rapport van de Privacy-werkorganisatie[1]. Het rapport is door de Privacy-werkorganisatie geschreven ten behoeve van het Universitair Medisch Centrum Groningen (in het vervolg UMCG). Dit rapport geeft namelijk een uiteenzetting van conclusies en aanbevelingen om het UMCG te laten voldoen aan de toekomstige Europese Privacy Verordening (in het vervolg EPV). De EPV gaat namelijk mogelijk van kracht in 2015 en wordt mogelijk per 2017 gehandhaafd. De aanbevelingen en conclusies met betrekking tot contractbeheer zijn voor dit onderzoek relevant. Dit onderzoek richt zich namelijk op het contractbeheer van het UMCG. Bij de implementatie van de EPV gaan werkprocessen veranderen en dat heeft gevolgen voor het handelen van de medewerkers van het UMCG, alsook het contractbeheer. Het contractbeheer binnen de centrale organisatieonderdelen van het UMCG voldoet namelijk op het moment niet aan de EPV.[2] Bij de sectoren/ afdelingen van het UMCG is daarom nog onduidelijk op welke wijze het contractbeheer per sector/ afdeling wordt vormgegeven. Het UMCG wil daarom de huidige situatie binnen de sectoren/ afdelingen graag weten, gezien het wil voldoen aan de EPV. Het UMCG wil namelijk graag betrouwbaar zijn omtrent de bescherming van persoonsgegevens. Daarnaast wil het onrechtmatige en onzorgvuldige omgang met gevoelige gegevens voorkomen, dan wel (nadelig) gevolgen daarvan beperken. Als de EPV niet wordt nageleefd door het UMCG, bestaat de (grote) kans dat er een sanctie wordt opgelegd door een toezichthouder.

Het doel van dit onderzoek is het doen van aanbevelingen aan het hoofd van de Umc-staf Juridische Zaken en aan de Privacy-werkorganisatie van het UMCG over hoe het contractbeheer binnen de sectoren/ afdelingen van het UMCG (opnieuw) kan worden ingericht om het UMCG compliant te maken aan de Europese Privacy Verordening en waarbij de belangen van verschillende sectoren/ afdelingen binnen het UMCG in acht worden genomen

De centrale onderzoeksvraag is:
Op welke wijze kan opnieuw binnen de sectoren/ afdelingen van het UMCG het contractbeheer worden ingericht, met de Europese Privacy Verordening als uitgangspunt en rekening houdend met de verschillende belangen van de sectoren/ afdelingen binnen het UMCG?

De deelvragen zijn:
- Wat is vastgelegd in de huidige wetgeving betreffende privacybescherming met betrekking tot verwerking van persoonsgegevens in contracten?
- Wat is vastgelegd in de nieuwe Europese Privacy Verordening met betrekking tot contracten?
- Waar dient een compliant contract met als uitgangspunt de Europese Privacy Verordening aan te voldoen?
- Wat wordt gesteld belangrijk te zijn uit de (juridische) literatuur omtrent de gevolgen van de Europese Privacy Verordening?
- Wat is bekend in de literatuur over contractbeheer?
- Wat is volgens de (juridische) literatuur een goede methode om nieuwe wet- en regelgeving binnen een organisatie te implementeren?
- Wat zijn de belangen van de sectoren/ afdelingen van het UMCG met betrekking tot een goede implementatie van de Europese Privacy Verordening?
- Welke soorten contracten sluiten de verschillende sectoren/ afdelingen van het UMCG?
- Hoe kan het UMCG per 1 september 2015 ervoor zorgen dat alle (nieuwe) contracten, met in achtneming van de Europese Privacy Verordening, compliant kunnen worden gesloten?
- Wat is de huidige infrastructuur van het contractbeheer binnen de sectoren/ afdelingen van het UMCG en hoe kan dat idealiter functioneren?
- Wat levert de vergelijking op van de resultaten van de deelvragen gericht op de theorie met de resultaten van de deelvragen gericht op de praktijk?

[1] De Privacy-werkorganisatie is onderdeel van het UMCG en belast met de doelstelling om het UMCG EPV-compliant te maken.
[2] *Rapport Privacy-werkorganisatie 'Implementatie EPV' versie 2.0, 2015.*

- Welke conclusies kunnen worden getrokken na vergelijking van de theorie en de praktijk?
- Welke aanbevelingen kunnen worden gedaan na vergelijking van de theorie en de praktijk?

De conclusie van dit onderzoek luidt:
Met de komst van de EPV zijn organisaties genoodzaakt om de bedrijfsvoering op bepaalde punten aan te passen om compliant te worden aan de EPV. Het UMCG is één van de organisaties die graag compliant wil worden aan de EPV. Hier moeten een aantal zaken voor veranderen, waaronder het contractbeheer. De EPV kan geïmplementeerd worden door het toepassen van de compliancecyclus. Om de compliancecyclus goed te realiseren zijn de omgevingsfactoren van belang. Commitment en de onvoorwaardelijke support van de Raad van Bestuur en de Umc-staf zijn daarom voor het compliancetraject van groot belang. Contractbeheer is één van de zaken die moet worden aangepast binnen het UMCG. Eén van de belangrijkste eisen van de EPV is het hebben van overzicht en inzicht in de gegevensverwerkingen. Contractbeheer kan worden gebruikt als instrument om dat te bewerkstelligen. De conclusie van het onderzoek is dat op het moment geen goed genoeg functionerend contractbeheer is binnen het UMCG om te kunnen voldoen aan de EPV. Dit kan mogelijk verklaard worden door de huidige manier van contractenadministratie en onduidelijke verantwoordlijkheden. Daarnaast wordt op het moment niet consequent gebruikgemaakt van de kennis en kunde van de staf Juridische Zaken om toekomstige contracten EPV-proof af te sluiten. Tot slot is binnen het UMCG bij mogelijk veel medewerkers niet duidelijk wie tekenbevoegd is. Dit kan leiden tot contracten die onbevoegd worden ondertekend. Hierdoor kan de onbevoegde ondertekenaar, en niet het UMCG, aansprakelijk worden gesteld. Ondanks de strenge eisen die de EPV stelt, biedt de verordening kansen voor het UMCG om te veranderen en mogelijkheden om de huidige manier van contractbeheer anders in te richten/ te verbeteren. Bij de implementatie van de EPV binnen het UMCG moeten de belangen van het UMCG als organisatie, alsook de belangen van de sectoren/ afdelingen worden meegenomen. Deze belangen zijn geïnventariseerd en luiden:

- Het UMCG heeft als organisatie de taak om te voldoen aan de wet- en regelgeving. Het imago van het UMCG hangt hiermee samen. Als het UMCG de EPV niet naleeft, betekent dat het UMCG de privacy omtrent gegevensverwerkingen niet op orde heeft en niet voldoende waarborgt. Aan de andere kant van een goed imago, staat het belang van kwaliteit. Vanuit het UMCG is er behoefte aan een goed functionerend contractbeheer, dit ten aanzien van compliancy, alsook uit financieel belang.
- De sectoren/ afdelingen hebben, net als het UMCG als organisatie, het belang dat ze moeten voldoen aan de wet- en regelgeving. Het imago van de sectoren/ afdelingen hangt hiermee samen. Bij een negatieve stempel kan dat de financiën schaden. Daarnaast is er vanuit de sectoren/ afdelingen behoefte aan duidelijkheid omtrent de (teken)bevoegdheden en behoefte aan verduidelijking omtrent welke gegevens zij wel en niet mogen inzien en verwerken.

De informatie uit het literatuuronderzoek en het praktijkonderzoek hebben geleid tot een aantal aanbevelingen, die mede door de conclusie, een antwoord geven op de centrale onderzoeksvraag. De volgende (sterk samengevatte) aanbevelingen zijn geformuleerd:

1. Om EPV compliancy te realiseren binnen het UMCG, is het eerst noodzakelijk om privacybewustwording ten aanzien van gegevensverwerking te creëren. Daarnaast dienen beleidsontwikkelingen omtrent de EPV te worden gepubliceerd op het UMCG intranet en directe betrokkenen dienen op de hoogte worden gesteld door middel van e-mail.

2. De wijzigingen van de EPV kunnen met behulp van de compliancecyclus binnen het UMCG worden geïmplementeerd en worden toegepast binnen het contractbeheer.

3. Op het moment is er geen goed functionerend contractbeheer aanwezig binnen de sectoren/ afdelingen van het UMCG. Allereerst moet er een inventarisatie van alle contracten binnen de sectoren/ afdelingen worden gehouden. Immers, zonder een goed overzicht van alle contracten kan er geen contractbeheer worden gecreëerd en kan niet worden voldaan aan de EPV.

4. Om professioneel contractbeheer te realiseren wordt aanbevolen goed beleid te schrijven en de 14 fasen van het contractbeheerproces in acht te nemen.

5. Het contractbeheerbeleid moet actief worden nageleefd door de medewerkers van het UMCG. Dit is van groot belang om het project 'implementatie contractbeheer' te laten slagen.

6. Om per 1 september 2015 contracten EPV-proof af te sluiten wordt aanbevolen om een eenvoudige juridische checklist op te laten maken door de staf Juridische Zaken en/of de Privacy-werkorganisatie.

7. Contracten die compliant zijn aan de EPV kunnen worden gerealiseerd door een goede samenwerking tussen de sectoren/ afdelingen en de staf Juridische Zaken.

8. Binnen de sectoren/ afdelingen wordt vaak gewerkt met eenzelfde soort contract per onderwerp. Op het moment worden daar vaak standaardcontracten voor gebruikt. Deze voldoen echter niet aan de EPV. De standaardcontracten moeten daarom worden herzien, zodat ze voldoen aan de EPV.

9. Binnen het UMCG is bij mogelijk veel medewerkers niet duidelijk wie tekenbevoegd is. Dit kan leiden tot contracten die onbevoegd worden ondertekend. Hierdoor kan de onbevoegde ondertekenaar, en niet het UMCG, aansprakelijk worden gesteld. Om dit te voorkomen moet nadrukkelijk worden benadrukt bij de controllers, afdelingshoofden en afdelingsmanagers etc. binnen de sectoren/ afdelingen, dat de huidige situatie van contractondertekening niet meer kan.

10. Naast contractbeheer wordt aanbevolen om contractmanagement in te richten. Dit om het contractbeheer te borgen. In nauwe samenwerking met de disciplines: de staf Financiën & Control, de staf Juridische Zaken en Inkoop kan een goed contractmanagementplan worden opgezet.

11. Tot slot wordt aanbevolen om vervolgonderzoek te houden dat zich richt op de situatie binnen alle afdelingen van de sectoren A tot en met F.

Met deze aanbevelingen kan het UMCG de eerste stap zetten om compliant te worden aan de EPV. De EPV gaat mogelijk per 01-01-2017 gehandhaafd worden. Het UMCG moet voor die tijd de nodige handelingen hebben verricht om compliancy te bewerkstelligen. Daarnaast kan het UMCG met in achtneming van de aanbevelingen een goed functionerend contractbeheer realiseren. Mocht het zo zijn dat de EPV uiteindelijk toch niet wordt gerealiseerd, dan kunnen de aanbeveling omtrent het contractbeheer wel worden gebruikt om het huidige contractbeheer te professionaliseren.

1 Inleiding

1.1 Onderzoekskader en interventiecyclus

1.1.1 Aanleiding

Binnen de Europese Unie heeft eenieder het fundamentele recht op een persoonlijke levenssfeer en de daarbij horende bescherming van persoonsgegevens. Organisaties die werken met persoonsgegevens dienen gehoor te geven aan wet- en regelgeving omtrent de privacy. Zij hebben de plicht om zorgvuldig
met persoonsgegevens om te gaan. Tegenwoordig is deze plicht voor organisaties, gevestigd in Nederland, vastgelegd in de Wet bescherming persoonsgegevens (in het vervolg Wbp). De Wbp is gebaseerd op de Databeschermingsrichtlijn (Richtlijn 95/46/EG) d.d. 1995. In 2010 heeft Eurocommissaris Viviane Reding kenbaar gemaakt dat zij de Europese privacyregels wilde herzien.[3] De huidige wetgeving sluit namelijk niet voldoende aan op de nieuwe technologieën waar informatie mee wordt ingewonnen. De Europese Commissie kwam daarom op 25 januari 2012 met het voorstel voor een nieuwe verordening: de Europese Privacy Verordening (in het vervolg EPV). Het doel van de verordening is de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en het vrije verkeer van die gegevens.[4]

De EPV is voorgesteld door de Europese Commissie, gezien de Richtlijn 95/46/EG d.d. 1995 verouderd is. Door de veroudering van de richtlijn, kan gesteld worden dat de Wbp dat logischerwijs ook is. Immers de Wbp is de Nederlandse uitwerking van de Richtlijn 95/46/EG. Naar verwachting zal de Wbp voor het grootste gedeelte worden ingetrokken. De EPV staat als verordening namelijk hoger in rang. Mogelijk gaat de EPV in 2015 van kracht en wordt twee jaren later gehandhaafd in 2017. De EPV is een verordening die hoge eisen gaat stellen aan de omgang met, en verwerking van alle persoonsgegevens binnen de zorg, het onderzoek, het onderwijs en in algemene zin van de bedrijfsvoering. Kort om, de EPV gaat impact hebben op de bedrijfsvoering van het Universitair Medisch Centrum Groningen (in het vervolg UMCG). Het UMCG werkt dagelijks met gevoelige gegevens betreffende patiënten, medewerkers etc. waarvan de veiligheid gewaarborgd moeten worden. Omtrent voornoemde is door de Raad van Bestuur op 22 april 2014 het 'Project Initiatie Document Europese Privacy Verordening' goedgekeurd. In dit document staat beschreven welke stappen moeten worden gezet om het UMCG op een goede manier voor te bereiden op de nieuwe verordening. Uit de eerste fase van het project is in december 2014 een rapport gekomen met daarin een impact- en risicoanalyse. Het rapport is van belang, gezien het UMCG betrouwbaar wil zijn omtrent bescherming van persoonsgegevens. Daarnaast wil het onrechtmatige en onzorgvuldige omgang met gevoelige gegevens voorkomen, dan wel (nadelige) gevolgen daarvan beperken. Als de EPV namelijk niet wordt nageleefd door het UMCG bestaat de (grote) kans dat er een sanctie wordt opgelegd door een toezichthouder.[5]

Om het UMCG te laten voldoen aan de EPV moeten er de nodige stappen worden gezet. De belangrijkste verschillen met de huidige wetgeving en de EPV zijn dat er veel minder ruimte is voor toepassing van de criteria proportionaliteit en subsidiariteit en daarnaast dat de werkingssfeer een stuk breder is.[6] De EPV vraagt namelijk meer aantoonbaarheid, in vergelijking met de huidige wetgeving, van een organisatie met betrekking tot het overzicht en inzicht van persoonsgegevensverwerking. Een aantal belangrijke punten die de EPV met zich meebrengt zijn:

- Inzicht en overzicht in alle verwerkingen.
- Documentatieplicht.
- Functionaris voor de Gegevensbescherming is verplicht.
- Privacybeleid moet zijn opgesteld.
- Inbedding privacy moet in de hele organisatie.

[3] DDMA, 'Privacy Europa', 12 februari 2015, www.ddma.nl (zoek op Juridisch loket, dossiers, privacy Europa).
[4] Verordening (EU) 0011/2012.
[5] Zie § 4.10 & § 4.11.
[6] A.W. Duthler & A.J. Biesheuvel, *Het Europese privacyrecht in beweging*, Deventer: Uitgeverij Kluwer 2013.

- Meldplicht om datalekken bij het CBP en/of betrokkene te melden.
- Privacy en security by design en by default.
- Uitgebreidere rechten van betrokkenen.
- Mogelijkheid van sancties.

Op basis van de impact- en risicoanalyse van de Privacy-werkorganisatie[7] zijn aanbevelingen geformuleerd. De aanbevelingen met betrekking tot contractbeheer zijn voor dit onderzoek van belang. Dit onderzoek richt zich namelijk op het contractbeheer van het UMCG. Bij de implementatie van de EPV gaan werkprocessen mogelijk veranderen en dat heeft gevolgen voor het handelen van medewerkers van de verschillende sectoren/ afdelingen, alsook het contractbeheer. Het contractbeheer voldoet namelijk mogelijk op het moment van schrijven niet aan de EPV.[8] Het onderzoek is daarom van belang, omdat de Privacy-werkorganisatie in de inventarisatie betreffende contracten en contractbeheer tot nu toe andere onderdelen heeft onderzocht dan de sectoren/ afdelingen. Bij de sectoren/ afdelingen is daarmee nog onduidelijk op welke wijze het contractbeheer per sector/ afdeling wordt vormgegeven.

1.1.2 De interventiecylus

Om een bestaande praktijksituatie te veranderen kan onderzoek als methode worden gebruikt om dat te bewerkstelligen. De methode van dit onderzoek kan getypeerd worden als praktijkgericht onderzoek. Dit, gezien praktijkgericht onderzoek als doel heeft een bijdrage te leveren aan een interventie om een bestaande praktijksituatie te veranderen. Om de praktijksituatie te veranderen kan het handelingsprobleem worden opgelost door middel van het doorlopen van een aantal fasen die zijn opgenomen in de interventiecyclus. Binnen de interventiecyclus zijn een vijftal fasen te onderscheiden:

1. *Probleemanalytisch onderzoek*
   In de probleemanalyse wordt gekeken naar wat nou precies het probleem is, waarom het een probleem is en wiens probleem het is. De fase van probleemanalyse moet ervoor zorgen dat alle betrokkenen duidelijkheid en zo mogelijk consensus creëren over de problematiek. De problematiek beheerst in deze de vraag van de organisatie, waaruit nu precies de gewraakte feitelijke situatie uit bestaat en welke toestand men expliciet wenst of impliciet in gedachte heeft. De uiteindelijke doelstelling van de probleemanalyse fase is bewustmaking, agendasetting en/of consensusvorming.
2. *Diagnostisch onderzoek*
   Als het probleem herkend en erkend is door alle betrokkenen, dan volgt de fase van diagnostiek. In de diagnostische fase worden de achtergronden en het ontstaan van de gesignaleerde problematiek bestudeerd. De inzichten die daaruit voortvloeien kunnen een mogelijke oplossing aanwijzen.
3. *Ontwerpgericht onderzoek*
   Uit de voorafgaande fasen, de probleemanalyse en de diagnose zijn punten gekomen om te komen tot een interventieplan om het handelingsprobleem op te lossen. In de ontwerpfase kan specifiek vorm worden gegeven door onderscheid te maken in vier vereisten: functionele, contextuele, gebruikers-, en structurele vereisten.
4. *Verandergericht onderzoek*
   Als het plan is ontworpen voor de organisatie dan moet deze worden geïmplementeerd binnen de desbetreffende organisatie. In de interventie/ verandering fase kan worden onderzocht welke knelpunten er zijn in de uitvoering, of er veranderingen noodzakelijk zijn in het plan van aanpak of dat alles naar behoren (koerscorrectie) loopt, door het verzamelen van gegevens over de uitvoering.
5. *Evaluatieonderzoek*
   Tijdens de evaluatiefase wordt de voorlopig laatste vraag beantwoord in hoeverre sprake is geweest van een geslaagde actie, of het probleem daadwerkelijk is opgelost. Er wordt wederom gekeken naar de feitelijke situatie en de gewenste situatie van de organisatie. In de evaluatiefase wordt dus bekeken in hoeverre in de verwachtingen van de betrokkenen in vervulling zijn gegaan. Als blijkt dat de verwachting niet geheel voldoen, tekortkomingen, dan kan men kijken hoe het in de toekomst verbeterd kan worden.[9]

[7] De Privacy-werkorganisatie is onderdeel van het UMCG en belast met de doelstelling om het UMCG EPV-compliant te maken.

[8] *Rapport Privacy-werkorganisatie 'Implementatie EPV' versie 2.0, 2015.*

[9] P. Verschuren & H. Doorewaarde, *Het ontwerpen van een onderzoek*, Den Haag: Boom Lemma Uitgevers 2007.

Het onderzoek zal dus plaatsvinden in één van de vijf fasen van de interventiecyclus. Dit onderzoek zal plaatsvinden in fase 3. In de impact- en risicoanalyse is namelijk al een probleemanalyse en diagnose geformuleerd.[10] Daarnaast wil het UMCG graag weten hoe de verordening kan worden geïmplementeerd (ontwerp).

1.1.3 Relevantie, opdrachtgever en actoren

Met de komst van de EPV is het UMCG verplicht om compliant[11] te worden aan de verordening. De verordening betreft namelijk Nederlandse wet- en regelgeving waar het UMCG aan moet en wil voldoen. Als het UMCG zich namelijk niet aan de verordening houdt, kan dat betekenen dat het UMCG een sanctie krijgt opgelegd. Als het UMCG het contractbeheer niet in overeenstemming met de EPV structureert, betekent dat voor het UMCG dat het niet compliant is. De relevantie van dit onderzoek is dan ook zeer sterk aanwezig.

De opdrachtgever voor dit onderzoek is de heer mr. R.E. Jager, hoofd Umc-staf Juridische Zaken.

Actoren die een rol spelen in het onderzoek zijn de verschillende sectoren/ afdelingen van het UMCG, die nader worden beschreven in paragraaf 1.2. Daarnaast de stuurgroep EPV die het project omtrent de nieuwe verordening in handen heeft genomen en tot slot de Privacy-werkorganisatie die belast is met de doelstelling om het UMCG EPV-compliant te maken.

1.1.4 Opvattingen actoren Europese Privacy Verordening

G.J. Brugman en R.J. Watson beiden advocaat bij Barents-Krans te Den Haag, benoemen dat er de komende jaren veel gaat veranderen op het privacygebied. Dit betekent dat 'ondernemingen' in heel Europa de komende jaren rekening zullen moeten houden met die regels en dat zij zich op moeten maken voor de nodige veranderingen. Het is daarom, zo stellen de advocaten, goed om de ontwikkelingen omtrent de verordening de komende tijd goed in de gaten te houden en de nodige proactieve houding aan te nemen om te veranderen.[12]

Victor Bouman, advocaat bij Wieringa advocaten, heeft in zijn artikel 'Privacy beter beschermd onder Europese Privacy Verordening' nader belicht wat de veranderingen zijn voor werkgevers en werknemers. Bouman schrijft als volgt; '*Alle bedrijven die met persoonsgegevens werken zullen te maken krijgen met een groot aantal nieuwe verplichtingen. Allereerst wordt het verplicht om het beleid rond de verwerking (het verzamelwoord voor elke handeling die met persoonsgegevens te maken heeft, zoals het verzamelen en bewaren daarvan) van persoonsgegevens transparant en eenvoudig toegankelijk te maken voor de personen waarvan de gegevens worden verwerkt (de "betrokkenen"). Ook zal dit beleid controleerbaar moeten zijn voor de privacy-autoriteit (in Nederland het CBP, dat binnenkort zijn naam wijzigt in Autoriteit persoonsgegevens). Uit de "privacy policy" zal onder meer moeten blijken welke persoonsgegevens worden verwerkt en waarom, alsmede welke maatregelen de onderneming heeft genomen om aan de wetgeving te voldoen.'* Voornoemde heeft dus ook direct betrekking op de sectoren/afdelingen van het UMCG, gezien zij veelvoudig met persoonsgegevens werken in bijvoorbeeld contracten. Daarnaast blijkt uit zijn bewoording dat '*wanneer er onverhoopt een beveiligingslek optreedt waardoor onbevoegden toegang krijgen tot persoonsgegevens, bijvoorbeeld door hacking, moet het bedrijf de privacy-autoriteit daarvan zo spoedig mogelijk in kennis stellen en maatregelen nemen, op straffe van eenzelfde hoge boete.'*[13]

De Koninklijke Nederlandsche Maatschappij tot bevordering der Geneeskunst (KNMG) vroeg zich het volgende af: *De Europese Unie bereidt nieuwe regels voor ter bescherming van persoonsgegevens, die ook hun impact zullen hebben op de zorg. Wat betekenen ontwikkelingen als een*

[10] *Rapport Privacy-werkorganisatie 'Implementatie EPV' versie 2.0, 2015.*

[11] Compliant is een begrip waarmee wordt aangeduid dat een persoon of organisatie werkt in overeenstemming met de geldende wet- en regelgeving.

[12] G.J. Brugman & R.J. Watson, 'De nieuwe privacy verordening, *De Hypotheekadviseurs 2013,* p.47.

[13] V. Bouman, 'Privacy beter beschermd onder Europese privacy-verordening' Wieringa Advocaten 3 december 2014,www.wieringa-advocaten.nl (zoek op Europese privacy, weblog, Victor Bouman 03/12/2014), geraadpleegd op 17 februari 2015.

'meldplicht datalekken' en het aanstellen van een privacy-functionaris voor de zorg?[14] De KNMG en de Nederlandse Vereniging van Ziekenhuizen (NVZ) verwachten de volgende veranderingen:

- wie patiëntgegevens verwerkt (de "verantwoordelijke") 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;[15]
- 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;
- de nationale toezichthouder (thans: 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.[16]

1.1.5 Eerder onderzoek over het onderwerp

Uit het project 'Implementatie EPV' is een rapport voortgekomen met daarin een impact- en risicoanalyse. Dit rapport is opgesteld door de Privacy-werkorganisatie.[17] Uit de impact- en risicoanalyse is geconstateerd dat het UMCG op het moment niet voldoet aan de EPV. Uit de inventarisatie van het rapport, ten aanzien van contractbeheer, zijn de volgende conclusies gekomen:

- Binnen de centrale organisatieonderdelen van het UMCG is geen totaaloverzicht van alle contracten, waaronder contracten met derde partijen, die gegevens in opdracht van het UMCG verwerken.
- Het contractbeheer en –archivering wordt bij elk organisatieonderdeel anders gedaan.
- Het is niet eenduidig wie verantwoordelijk is voor een gegevensverwerking door een derde partij en voor het bijbehorende contract
- Het is niet geborgd dat nieuw te sluiten overeenkomsten met derden voldoen aan de eisen van de EPV.
- De kwaliteit van huidige contracten wat betreft vereisten Wbp/ EPV is zeer uiteenlopend.[18]

Geconcludeerd kan worden dat het contractbeheer binnen de centrale organisatieonderdelen van het UMCG anno 2015 erg versnipperd is. Het onderzoek dat de Privacy-werkorganisatie heeft verricht betreffende contracten en contractbeheer heeft zich met name gericht op de centrale organisatiedelen van het UMCG en niet op de sectoren/ afdelingen. Uitzondering daarop is sector A. Sector A is wel globaal onderzocht waaruit onder andere is gebleken dat het borgen van de privacy in sommige contracten niet wordt besproken, niet consequent en niet accuraat zijn vastgelegd. Bij de andere sectoren is het nog onduidelijk op welke wijze het contractbeheer wordt vormgegeven en of het wel of niet voldoet aan de toekomstige EPV.

1.2 Organisatiestructuur

Het UMCG is één van de grootste ziekenhuizen in Nederland en de grootste werkgever van Noord-Nederland met 11.968 werknemers.[19] Het UMCG heeft als missie het bouwen aan een toekomst van gezondheid. Om de missie te bewerkstelligen zijn er drie kerntaken geformuleerd: zorg, onderwijs en onderzoek.[20] De structuur van het UMCG is verdeeld in de Raad van Bestuur die is belast met de algemene leiding van het UMCG. De Raad van Toezicht is belast met het toezicht houden op de Raad van Bestuur.

---

[14] 'Nieuwe Europese privacyregels in aantocht', KNMG 23 mei 2014, www.knmg.artsennet.nl (zoek op Europese privacyregels), geraadpleegd op 16 februari 2015.

[15] 'Nieuwe Europese privacyregels in aantocht', KNMG 23 mei 2014, www.knmg.artsennet.nl (zoek op Europese privacyregels), geraadpleegd op 16 februari 2015.

[16] 'Privacy' NVZ, www.nvz-ziekenhuizen.nl (zoek op 'Europese privacyregels'), geraadpleegd op 17 februari 2015.

[17] *Rapport Privacy-werkorganisatie 'Implementatie EPV' versie 2.0,* 2015.

[18] *Rapport Privacy-werkorganisatie 'Implementatie EPV' versie 2.0,* 2015. p. 10-11.

[19] 'Feiten en cijfers' UMCG, www.umcg.nl (zoek op 'over het UMCG'), geraadpleegd op 9 juni 2015.

[20] 'Missie en visie' UMCG, www.umcg.nl (zoek op 'over het UMCG'), geraadpleegd op 9 juni 2015.

Naast voornoemde werkt het UMCG met een staf die werkzaam is ten behoeve van de Raad van Bestuur, de centrale organisatieonderdelen en de sectoren. Het UMCG is onderverdeeld in sectoren/ afdelingen. Er zijn in totaal zes sectoren: sector A *langdurige zorg/ vaten*, sector B *kortdurende zorg/ buik*, sector C *kinderen/ voortplanting/ revalidatie/ psychiatrie*, sector D *oncologie*, sector E *ondersteunde specialismen* en sector F *ontwikkeling/ overdracht* (zie bijlage 1: Organogram). De verschillende sectoren fungeren allen met een eigen management, toegekend budget etc. Er kan dus gesteld worden dat de sectoren/ afdelingen samen een deel van het gehele UMCG vormen, maar onderling apart fungeren naar de buitenwereld. De sectoren kunnen wellicht getypeerd worden als een bedrijfsbureau, wat mogelijk de versnipperdheid van het contractbeheer verklaard.

1.3 Afbakening onderzoek

Het onderzoek heeft zich gericht tot de situatie anno 2015 binnen de volgende sectoren van het UMCG:

- Sector A Langdurige zorg/ vaten
- Sector B Kortdurende zorg/ buik
- Sector C Kinderen/ voortplanting/ revalidatie/ psychiatrie,
- Sector D Oncologie
- Sector E Ondersteunde specialismen

1.4 Doelstelling

Het doel van dit onderzoek is:
Het doen van aanbevelingen aan het hoofd van de Umc-staf Juridische Zaken en de Privacy-werkorganisatie van het UMCG over hoe het contractbeheer binnen de sectoren/ afdelingen van het UMCG (opnieuw) kan worden ingericht om het UMCG compliant te maken aan de Europese Privacy Verordening en waarbij de belangen van verschillende sectoren/ afdelingen binnen het UMCG in acht worden genomen

door

het in kaart brengen van de wet- en regelgeving, het afnemen van interviews bij sectorcontrollers, het uitvoeren van een (juridisch en niet-juridisch) literatuuronderzoek, de huidige situatie van het contractbeheer bij de sectoren/ afdelingen van het UMCG en de gewenste situatie in kaart brengen, waarbij de belangen van de sectoren/ afdelingen en het belang van het UMCG in zijn totaliteit in acht worden genomen, met de Europese Privacy Verordening als uitgangspunt.

1.5 Onderzoeksvragen

1.5.1 Centrale onderzoeksvraag

Op welke wijze kan opnieuw binnen de sectoren/ afdelingen van het UMCG het contractbeheer worden ingericht, met de Europese Privacy Verordening als uitgangspunt en rekening houdend met de verschillende belangen van de sectoren/ afdelingen binnen het UMCG?

1.5.2 Deelvragen

1. Deelvragen gericht op 'theoretische' bronnen

- Wat is vastgelegd in de huidige wetgeving betreffende privacybescherming met betrekking tot verwerking van persoonsgegevens in contracten?
- Wat is vastgelegd in de nieuwe Europese Privacy Verordening met betrekking tot contracten?
- Waar dient een compliant contract met als uitgangspunt de Europese Privacy Verordening aan te voldoen?
- Wat wordt gesteld belangrijk te zijn uit de (juridische) literatuur omtrent de gevolgen van de Europese Privacy Verordening?
- Wat is bekend in de literatuur over contractbeheer?
- Wat is volgens de (juridische) literatuur een goede methode om nieuwe wet- en regelgeving binnen een organisatie te implementeren.

2. Deelvragen gericht op de praktijk (empirie)

- Wat zijn de belangen van de sectoren/ afdelingen van het UMCG met betrekking tot een goede implementatie van de Europese Privacy Verordening?

- Welke soorten contracten sluiten de verschillende sectoren/ afdelingen van het UMCG?

- Hoe kan het UMCG per 1 september 2015 ervoor zorgen dat alle (nieuwe) contracten, met in achtneming van de Europese Privacy Verordening, compliant kunnen worden gesloten?

- Wat is de huidige infrastructuur van het contractbeheer binnen de sectoren/ afdelingen van het UMCG en hoe kan dat idealiter functioneren?

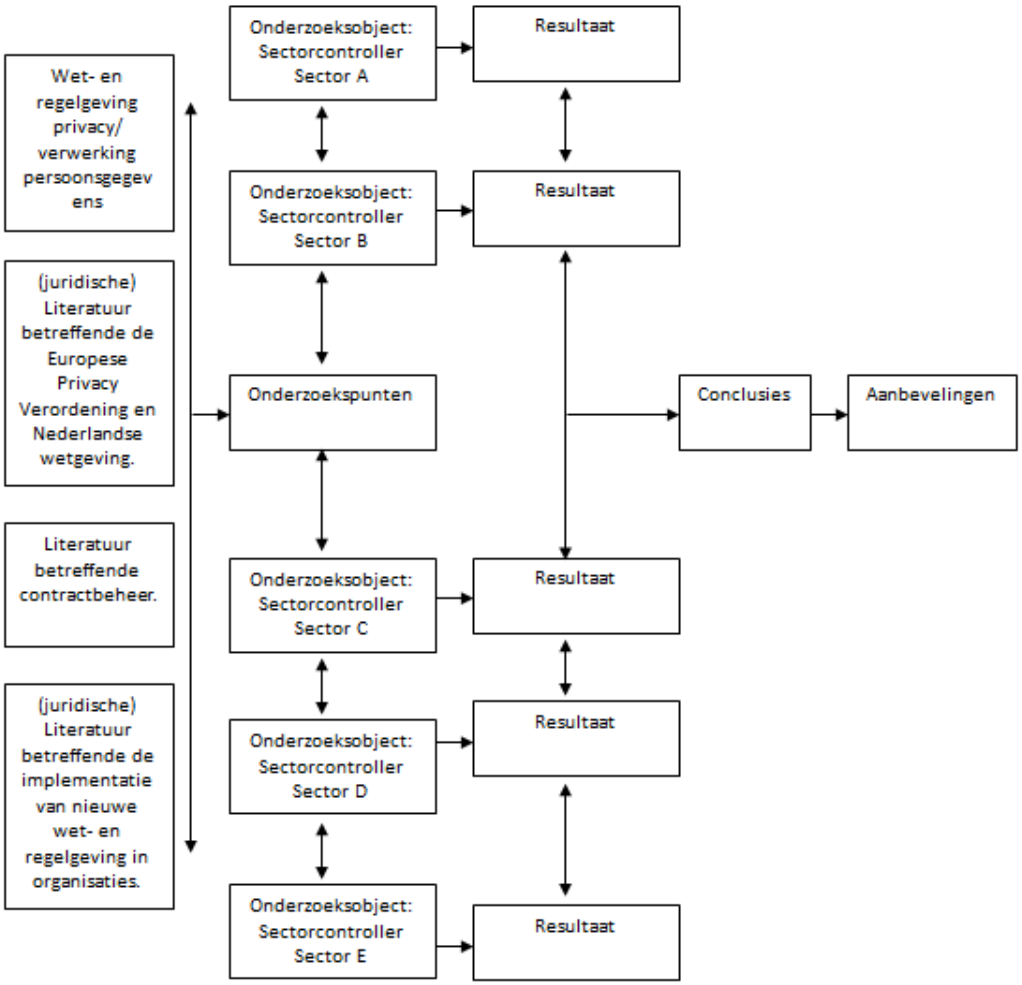
3. Deelvragen gericht op de analyse

- Wat levert de vergelijking op van de resultaten van de deelvragen gericht op de theorie met de resultaten van de deelvragen gericht op de praktijk?

- Welke conclusies kunnen worden getrokken na vergelijking van de theorie en de praktijk?

- Welke aanbevelingen kunnen worden gedaan na vergelijking van de theorie en de praktijk?

1.6 ONDERZOEKSMODEL



Figuur 1 Onderzoeksmodel

1.7 Leeswijzer

Dit rapport is verdeeld in een methodologische verantwoording, literatuuronderzoek, praktijkonderzoek, analyse, conclusie en wordt afgesloten met aanbevelingen.

De methodologische verantwoording is te vinden in hoofdstuk 2.

Het literatuuronderzoek is vervolgens te vinden in de hoofdstukken 3 tot en met 6. Deze hoofdstukken bevatten de volgende onderwerpen: de Wet bescherming persoonsgegevens (hoofdstuk 3), de Europese Privacy Verordening (hoofdstuk 4), hoe contractbeheer kan worden ingericht (hoofdstuk 5) en tot slot een methode om de Europese Privacy Verordening binnen het UMCG te kunnen implementeren (hoofdstuk 6).

Het praktijkonderzoek volgt na het literatuuronderzoek. Het praktijkonderzoek is daarom te vinden in de hoofdstukken 7 tot en met 9. Deze hoofdstukken bevatten de volgende onderwerpen: de huidige bevoegdheidsregeling binnen het UMCG (hoofdstuk 7), de praktijkresultaten (hoofdstuk 8) en tot slot een korte uiteenzetting van het praktijkonderzoek (hoofdstuk 9).

Na het praktijkonderzoek zijn de analyses geformuleerd in hoofdstuk 10, waarin de resultaten van het praktijkonderzoek zijn vergeleken met de theoretische inzichten omtrent de onderzoekspunten. Tot slot zijn de aanbevelingen en conclusie opgenomen in hoofdstuk 11.

De inleiding van dit onderzoek is hierbij beschreven, waardoor nu de stap kan worden gezet naar hoofdstuk 2. In hoofdstuk 2 worden de keuzes, die in het onderzoek gemaakt zijn, uiteengezet. Daarnaast bevat dit hoofdstuk een reflectie op het onderzoek.

2 METHODOLOGISCHE VERANTWOORDING

2.1 INLEIDING

In dit hoofdstuk volgt een uiteenzetting van de keuzes die gemaakt zijn in dit onderzoek. De methodologische verantwoording van dit onderzoek maakt transparant op welke wijze dit onderzoek is uitgevoerd. Er zijn namelijk verschillende methoden gebruikt voor dit onderzoek om de deelvragen te beantwoorden. Als eerste wordt het vooronderzoek beschreven (§ 2.2), daarna volgt het literatuuronderzoek (§ 2.3), het praktijkonderzoek (§ 2.4), de analyse, conclusie en aanbevelingen (§ 2.5), de kwaliteit van het onderzoek (§ 2.6) en tot slot wordt afgesloten met een reflectie (§ 2.7).

2.2 VOORONDERZOEK

In de eerste fase van het onderzoek is de onderzoeksopzet gerealiseerd. Gekozen is om direct te beginnen met de onderzoeksopzet, gezien de onderzoeker pas eind januari 2015 een organisatie had gevonden. Door het maken van een onderzoeksopzet (en niet een onderzoeksvoorstel) is een risico genomen, maar ook tijd gewonnen tijdens de intervisiegroepen. De onderzoeker heeft namelijk één intervisiegroep bijgewoond, waarna goedkeuring volgde van de toetsingscommissie. In de onderzoeksopzet zijn de volgende punten opgenomen: het onderzoekskader, de fase in de interventiecylus, de doelstelling van het onderzoek, de centrale onderzoekvraag, de deelvragen, onderzoeksmethoden, voorlopige literatuurbronnen en relevante wet- en regelgeving en tot slot het onderzoeksmodel.

2.3 LITERATUURONDERZOEK

In de tweede fase van het onderzoek is het literatuuronderzoek gerealiseerd, door het maken van een juridische inhoudsanalyse. De juridische inhoudsanalyse is tot stand gekomen door alle relevante rechtsbronnen en juridische literatuur te bestuderen. Er is door de onderzoeker geen jurisprudentie gebruikt in de onderzoek. Dit, omdat er over de Europese Privacy Verordening nog geen jurisprudentie is geschreven. Daarnaast was jurisprudentie voor de begrijpelijkheid van de Wet bescherming persoonsgegevens, in de ogen van de onderzoeker, niet noodzakelijk. Per theoretisch hoofdstuk wordt nu aangegeven waarom bepaalde keuzes zijn gemaakt. Het betreft de hoofstukken 3 tot en met 7.

- *Hoofdstuk 3*

In hoofdstuk 3 is door de onderzoeker gekozen om een juridische inhoudsanalyse te maken, door het gebruiken van relevante bronnen in het kader van de Wet bescherming persoonsgegevens. Over de Wet bescherming persoonsgegevens was een scala aan literatuur te vinden. De onderzoeker had daarom een ruime literatuurkeuze. Gekozen is om de boeken van de HanzeMediatheek Groningen te gebruiken. Dit, gezien de HanzeMediatheek zeer toegankelijk was voor de onderzoeker. Op basis van de deelvraag die is gesteld in het kader van de Wet bescherming persoonsgegevens heeft de selectie plaatsgevonden. De onderzoeker heeft echter niet alleen gebruikgemaakt juridische literatuur. Gekozen is ook om de desbetreffende wet goed te lezen. Hieruit is een selectie ontstaan m.b.t. alle relevante artikelen in het kader van overeenkomsten. Deze artikelen zijn verder gespecifieerd en omschreven met behulp van de Memorie van Toelichting Wbp. Na het schrijven van hoofdstuk 3 is gebleken dat dit hoofdstuk niet relevant is met het oog op mogelijke onderzoekspunten. Dit hoofdstuk is daarom ook met name geschreven ter ondersteuning van hoofdstuk 4: de Europese Privacy Verordening.

- *Hoofdstuk 4*

In hoofdstuk 4 is wederom door de onderzoeker gekozen om een juridische inhoudsanalyse te maken, door het gebruiken van relevante bronnen in het kader van de Europe-

se Privacy Verordening. De literatuur over deze verordening was echter niet in groten getale aanwezig. Dit kwam waarschijnlijk omdat de verordening vrij nieuw is. De onderzoeker heeft daarom met name gebruikgemaakt van de tekst uit de voorgestelde verordening en daarbij de amendementen van het Europees Parlement gelezen. Gekozen is voor dezelfde opzet als hoofdstuk 3. Niet alleen vanwege de leesbaarheid, maar ook omdat de onderzoeker in hoofdstuk 4, ten aanzien van de begrippen, veel verwijst naar de begrippen in hoofdstuk 3. Sommige begrippen zijn namelijk hetzelfde gebleven ten aanzien van de Wet bescherming persoonsgegevens, indien niet letterlijk verwoord dan toch qua strekking. Ondanks het feit dat de onderzoeker erg veel informatie uit de verordening kon halen, is ook gekozen om in juridische databases te zoeken. In de databases werd gezocht naar relevante artikelen omtrent de verordening. Deze artikelen waren niet zeer toegankelijk. Desondanks is de onderzoeker er in geslaagd om bepaalde juridische artikelen toe te passen in hoofdstuk 4. Deze juridische artikelen werden met name gebruikt om te kijken of de artikelen uit de verordening goed door de onderzoeker zijn geïnterpreteerd. De onderzoekspunten zijn geselecteerd op relevantie. Het UMCG wilde namelijk weten of het voldoet aan de verordening en had daarnaast een vraag omtrent de contracten. Voor de onderzoeker was het echter niet haalbaar om alle contracten juridisch te toetsen aan de verordening. Door de onderzoeker is daarom de keuze gemaakt om zich te richten op de standaardmodelovereenkomsten die het UMCG hanteert.

- *Hoofdstuk 5*

In hoofdstuk 5 is door de onderzoeker gebruikgemaakt van niet-juridische literatuur omtrent de inrichting van contractbeheer. Specifieke literatuur was erg moeilijk om te vinden. Door de onderzoeker zijn toch een aantal bronnen gevonden, waar gebruik van kon worden gemaakt, om de deelvraag omtrent contractbeheer goed te beantwoorden. De literatuur is daarom geselecteerd op het onderwerp 'het inrichten van contractbeheer'. Gezien het contractbeheer een belangrijke rol heeft in dit onderzoek zijn er verscheidende onderzoekspunten geformuleerd. Sommige onderzoekspunten zijn geformuleerd op verzoek van het UMCG. Het UMCG wilde graag weten hoe het contractbeheer binnen het UMCG functioneert en of dit idealiter kan functioneren. Daarnaast zijn door de onderzoeker onderzoekspunten geformuleerd op basis van aspecten die in de literatuur worden aangewezen als belangrijk. Zoals contracteren met derden, verantwoordelijkheid en autorisatie.

- *Hoofdstuk 6*

In hoofdstuk 6 is door de onderzoeker gebruikt gemaakt van juridische literatuur omtrent compliance en implementatie wet – en regelgeving. Wederom was het erg lastig om hier goede en duidelijke literatuur over te vinden. Tijdens de HBO-Rechten opleiding van de onderzoeker werd gebruikgemaakt van een boek met als deelonderwerp compliance en implementatie wet- en regelgeving. De onderzoeker vond dit boek zeer relevant ten aanzien van bepaalde methoden, zoals de compliancecyclus. Dit boek is daarom veel gebruikt in hoofdstuk 6. Daarnaast is nog een bron gebruikt die betrekking heeft op het risicomanagement in ziekenhuizen. De onderzoekspunten hadden met name betrekking op bewustwording. Daarnaast wilde de onderzoeker graag weten hoe het UMCG nieuwe wet- en regelgeving implementeert.
Voordat aan het praktijkonderzoek is begonnen, is het literatuuronderzoek helemaal afgerond. De onderzoeker heeft deze keuze gemaakt, omdat hij tijdens de interviews met de respondent verdiepend op de stof wilde ingaan en daardoor goed kon doorvragen. Het praktijkonderzoek is daarom pas tot stand gekomen nadat het theoretisch kader was afgerond.

2.4 Praktijkonderzoek

2.4.1 Deskresearch en gesprekken

In de derde fase van dit onderzoek is het praktijkgedeelte tot stand gekomen door het houden van beperkt deskresearch en gesprekken met medewerkers van het UMCG. Het deskresearch heeft zich toegespitst tot het lezen van rapportages geschreven door de Privacy-werkorganisatie, de bevoegdhedenregelingen en standaardcontractmodellen binnen het UMCG. Daarnaast zijn wederom de wetsartikelen van de Wet bescherming persoonsgegevens en de Europese Privacy Verordening grondig bestudeerd. Dit om aan te kunnen geven wat de verschillen zijn met betrekking tot veranderingen en gevolgen ten aanzien van contracten. Naast het deskresearch zijn gesprekken gevoerd met me-

dewerkers vanuit het UMCG die in het kader van dit onderzoek, de onderzoeker van relevantie informatie konden voorzien. De onderzoeker had namelijk informatie nodig over welke soorten contracten het UMCG gebruikt en de werking van de bevoegdhedenregelingen in de praktijk. Met de volgende personen is gesproken, gezien zij actief waren in projecten, of actief zijn in lopende projecten in het kader van contracten:

Naam	Functie
Werknemer 1	Teamleider UMC-staf/Bureau Inkoop
Werknemer 2	Kwaliteitsfunctionaris UMC-staf/Bureau Inkoop
Werknemer 3	Beleidsmedewerker UMC-staf Beleid

Tabel 1 UMCG medewerkers

2.4.2 Interviews

In het praktijkgedeelte van dit onderzoek is naast deskresearch, ook een kwalitatief onderzoek uitgevoerd. Kwalitatief onderzoek geeft een diepgaand subjectief inzicht over de achterliggende motivaties, meningen, wensen en behoeften van de onderzoeksdoelgroep.[21] Voor dit onderzoek is kwalitatief onderzoek gekozen, omdat het naast het diepgaande inzicht, ook kan worden ingezet om de respondenten zelf te laten meedenken. Bijvoorbeeld over hoe het huidige contractbeheer functioneert en hoe dit idealiter kan functioneren. Daarnaast is er voor kwalitatief onderzoek gekozen om de respondenten mee te laten denken over de invulling van toekomstig beleid. De onderzoeker wilde namelijk graag weten wat de ervaringen en belangen van de respondenten zijn ten aanzien van contractbeheer en de Europese Privacy Verordening.

Gekozen is om de sectoren A tot en met E van het UMCG te onderzoeken, gezien zij relevant bleken te zijn in het kader van gegevensverwerkingen en contractbeheer. Sector F blijft daarom over en is niet onderzocht. Deze keuze is na gedegen overleg met de Privacy-werkorganisatie gemaakt, gezien sector F in het kader van gegevensverwerkingen minder relevant bleek te zijn. Tot slot zijn de afdelingen niet grondig onderzocht en geanalyseerd. Deze keuze is gemaakt om het onderzoek in te kaderen en haalbaar te maken binnen het daarvoor beschikbare tijdbestek van vier maanden.

De selectieve groep respondenten die hebben meegewerkt aan dit onderzoek zijn geselecteerd om hun positie en functie binnen het UMCG:

Naam	Functie
Respondent 1	Controller sector A
Respondent 2	Controller sector A
Respondent 3	Controller sector B
Respondent 4	Controller sector C
Respondent 5	Controller sector D
Respondent 6	Controller sector E

Tabel 2 Respondenten

Deze personen zijn in eerste instantie gekozen omdat zij de doelgroep vormen van dit onderzoek. Het onderzoek richt zich namelijk op de sectoren/ afdelingen van het UMCG. Daarnaast is gekozen voor deze personen, gezien zij allen vanuit hun functie geacht worden om op de hoogte te zijn betreffende de situatie binnen de eigen sector en daarmee binnen de onderliggende afdelingen. Tot slot is voor deze personen gekozen om een eerste bewustwording van de Europese Privacy Verordening te creëren op sectorniveau.

In totaal zijn er vijf interviews afgenomen, waarvan er bij twee interviews met twee personen tegelijk werd gesproken en bij drie interviews individueel. In totaal waren er daarom zeven respondenten. Aan alle respondenten zijn dezelfde soort vragen gesteld. Ten eerst zijn vragen gesteld over de contracten die worden gesloten binnen de sectoren/ afdelingen en wie daarvoor verantwoordelijk is. Ten tweede zijn vragen gesteld over hoe de sector/ afdelingen kan voldoen aan de Europese Privacy Verordening en de risico's binnen de sector/ afdelingen met betrekking tot privacywetgeving in contracten. Ten derde zijn vragen gesteld over wat de huidige infrastructuur van het contractbeheer is binnen de sector/ afdelingen en hoe dit idealiter kan functioneren. Tot slot zijn aan alle respondenten vragen gesteld over de belangen in het kader van contractbeheer en de Europese Privacy Wetgeving. (zie bijlage 2 voor de interviewvragen)

[21] Right marktonderzoek, www.rightmarktonderzoek.nl (zoek op 'methoden onderzoek'), geraadpleegd op 22 mei 2015.

Om alle ervaringen, ideeën en meningen goed te kunnen verzamelen is gebruikgemaakt van een halfgestructureerd interview, bestaande uit gesloten en open vragen. De interviewer heeft waar mogelijk doorgevraagd. De interviews zijn, na toestemming van alle respondenten, opgenomen met behulp van een dictafoon. De hieruit voorvloeiende geluidsopnamen zijn zo volledig mogelijk uitgeschreven en de transcripties die hieruit voorkwamen zijn geanalyseerd en vervolgens per uitspraak gegroepeerd. De gegroepeerde uitspraken zijn vervolgens bij elkaar gezet en verwerkt per thema in hoofdstuk 8.

2.5 Analyse, conclusie en aanbevelingen

De analyse is tot stand gekomen door de praktijkresultaten en theoretische inzichten omtrent de onderzoekspunten te vergelijken. Door de vergelijking van de praktijk en theorie kon een eindconclusie worden getrokken. Hierdoor konden, naar organisatiebehoefte, de aanbevelingen worden geformuleerd. Dit alles heeft uiteindelijk geleid tot de beantwoording van de centrale onderzoeksvraag en is de doelstelling van het onderzoek behaald.

Om voornoemde te bewerkstelligen is door de onderzoeker gekozen het volgende proces door te lopen. Ten eerste zijn de onderzoekspunten gegroepeerd in de thema's: compliance en implementatie EPV, contractbeheer binnen de sectoren/ afdelingen, contracteren binnen het UMCG en autorisatie. De inhoud van deze thema's zijn tot stand gekomen door gebruik te maken van de uitspraken van de respondenten. Daarnaast zijn de bevindingen van de onderzoeker tijdens het deskresearch en de informele gesprekken gebruikt. Deze resultaten zijn gekoppeld aan de theoretische inzichten. Door de praktijk en de theorie de vergelijken kon een korte analyse per thema worden gemaakt. Uiteindelijk kon de onderzoeker een conclusie trekken en zijn de aanbevelingen geformuleerd.

2.6 Kwaliteit van het onderzoek

Het nadeel van kwalitatief onderzoek is dat de resultaten niet altijd statistisch representatief zijn, maar een indicatie geven van wat er leeft onder de ondervraagde respondenten.[22] De respondenten waren qua functie en aantal representatief. Dit, omdat de sectoren worden gemanaged door de controllers. Controllers worden allen vanuit hun functie geacht om op de hoogte te zijn van de situatie binnen de eigen sector en daarmee binnen de onderliggende afdelingen.

Wat betreft de betrouwbaarheid van de uitspraken in de interviews, moet worden vastgesteld of deze intersubjectief waren. Het is hierbij van belang dat wordt vastgesteld of de interviewer invloed heeft gehad op de resultaten. De interviewer heeft getracht zo objectief mogelijk te blijven door zich niet te laten beïnvloeden door uitspraken van reeds geïnterviewde respondenten. Daarnaast heeft de interviewer ook getracht zich niet te laten beïnvloeden op basis van reeds opgedane ervaringen en vooroordelen. De objectiviteit is zo goed mogelijk bewerkstelligd door gebruikt te maken van een vooraf opgestelde vragenlijst en daarnaast de respondenten zo veel mogelijk aan het woord te laten. De objectiviteit is echter bij de interviewer enigszins in het geding geraakt, doordat de interviewer mogelijk opgedane kennis heeft meegenomen naar de daaropvolgende interviews. Dit heeft mogelijk een beperkte invloed gehad, gezien de situatie binnen de sectoren nagenoeg overal hetzelfde bleek te zijn. Dit blijkt uit de keuze om alles te transcriberen, waardoor de verhalen van de respondenten goed in kaart zijn gebracht en daarom weinig tot geen informatie verloren is gegaan.

2.7 Reflectie op het onderzoek

Dit uitgevoerde onderzoek ken haar kwaliteiten en beperkingen. De lezer dient hier daarom rekening mee te houden bij de waardering van de onderzoeksresultaten en de gegeven conclusie en aanbevelingen. Eén van de kwaliteiten van dit onderzoek is dat het onderzoek is gehouden binnen bijna alle sectoren van het UMCG. Uitzondering daarop is sector F. Ondanks deze uitzondering zijn de successen van de inventarisatie van de huidige situatie binnen de sectoren/ afdelingen A tot en met E, ten aanzien van de Europese Privacy Verordening en het contractbeheer heel concreet.

[22] Right marktonderzoek, www.rightmarktonderzoek.nl (zoek op 'methoden onderzoek'), geraadpleegd op 22 mei 2015.

Daarnaast is een kwaliteit van het onderzoek, de theoretische uiteenzetting. De deelvragen zijn allemaal heel specifiek beantwoord in het kader van overeenkomsten en compliance. Hierdoor kan het onderzoek als aanknopingspunt functioneren voor een vervolgonderzoek. Een vervolgonderzoek wordt ook aanbevolen door de onderzoeker. Immers de afdelingen binnen de sectoren zijn niet grondig onderzocht. Er is namelijk uitgegaan van de kennis van de respondenten. Gezien zij vanuit hun functie geacht worden om de situatie binnen de afdelingen te kennen. Dit is ook meteen een knelpunt van dit onderzoek, gezien de onderzoeker zich voornamelijk heeft gericht op de sectoren. De onderzoeker had zich nog wel willen richten tot bepaalde afdelingen binnen de sectoren. Tijdens het onderzoek werd echter door de onderzoeker geconstateerd, dat het interviewen van respondenten binnen de afdelingen niet meer haalbaar was in de resterende tijdsperiode.

Het is de onderzoeker ook bijna gelukt om volgens de planning te werken. Achteraf heeft de onderzoeker erg veel tijd besteed aan het theoretische kader van dit onderzoek. Dit had de onderzoeker anders moeten inplannen. Dit heeft met name gelegen aan het feit dat de onderzoeksopzet in februari 2015 tot stand is gekomen. Hierdoor is bijna 25% van het onderzoek gericht geweest op de opzet. Ondanks het feit dat de onderzoeksopzet snel goed is gekeurd, is hier wellicht te veel tijd in gestoken. Desondanks zijn de onderzoeksvragen allemaal naar wens van de onderzoeker opgelost.
Tot slot is de grote waarde van dit onderzoek, dat er langzamerhand EPV bewustwording wordt gecreëerd binnen de sectoren/ afdelingen van het UMCG.

In de volgende hoofstukken is het theoretisch kader van dit onderzoek uiteengezet. Ingegaan wordt op de huidige en nieuwe wetgevingen omtrent de verwerking van persoonsgegevens. Vervolgens treft u een methode aan om contractbeheer in te richten en tot slot een manier om nieuwe wet- en regelgeving binnen een organisatie te implementeren.

3 WET BESCHERMING PERSOONSGEGEVENS

3.1 INLEIDING

In dit hoofdstuk volgt de eerste uiteenzetting van de theorie. Dit hoofdstuk richt zich op het formuleren van een antwoord op de eerste theoretische deelvraag en luidt:

- *Wat is vastgelegd in de huidige wetgeving betreffende privacybescherming met betrekking tot verwerking van persoonsgegevens in contracten?*

Achtereenvolgens worden de volgende onderwerpen besproken: geschiedenis (§ 3.2), reikwijdte (§ 3.3), beginselen Wbp (§ 3.4), belangrijke begrippen (§ 3.5), verwerken van medische persoonsgegevens (§ 3.6), toezicht en handhaving (§ 3.7) en tot slot de conclusie (§ 3.8). Deze theoretische uiteenzetting mondt niet uit in een aantal onderzoekspunten. Dit hoofdstuk is namelijk geschreven om de lezer kennis te laten maken met de huidige wetgeving en tevens om het volgende hoofdstuk 4 goed te kunnen begrijpen. Dit hoofdstuk dient daarnaast ter ondersteuning van hoofdstuk 4 m.b.t. de beginselen en de begrippen.

3.2 GESCHIEDENIS

De Wbp d.d. 2001 is de opvolger van de Wet persoonsregistratie (in het vervolg Wpr) d.d. 1989. De reden voor het in het leven roepen van de Wbp is ten eerste de Richtlijn 95/46/EG betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. De Wbp is de Nederlandse uitwerking van die richtlijn. Door middel van de Europese richtlijn trachtte de Europese Unie (1995) de wetgeving betreffende de bescherming van de persoonsgegevens te harmoniseren. [23] Elke lidstaat hanteerde namelijk andere privacywetgeving. De nadelige effecten van die uiteenlopende privacywetten waren met name een belemmering voor de uitwisseling van persoonsgegevens. Naast de richtlijn was er nog een reden voor Nederland om de Wbp in het leven te roepen. In het jaar 2000 gold de Wpr namelijk al tien jaar, reden voor een tweetal evaluaties. De Wpr was geëvalueerd en er kwam naar voren dat de Wpr niet meer aansloot bij de dagelijkse praktijk van gegevensverwerking.[24] Tegenwoordig zijn de algemene regels betreffende omgang met persoonsgegevens opgenomen in de Wbp. In de Wbp staat namelijk wat er allemaal wel en niet mag m.b.t. verwerking van persoonsgegevens.[25] Vervolgens kan door deze korte uiteenzetting van de geschiedenis, de stap worden gemaakt naar de reikwijdte van de Wbp.

3.3 REIKWIJDTE

De reikwijdte van de Wbp wordt bepaald door de artikelen 2, 3 en 4 Wbp. De materiële reikwijdte beslaat de geheel of gedeeltelijk geautomatiseerde verwerkingen van persoonsgegevens, alsmede de niet-geautomatiseerde verwerkingen van persoonsgegevens die in een bestand zijn opgenomen, of bestemd zijn om daarin te worden opgenomen.[26] Artikel 3 Wbp voegt hieraan toe dat de Wbp niet van toepassing is op de verwerking van persoonsgegevens voor uitsluitend journalistieke, artistieke of literaire doeleinden. Het geografische toepassingsgebied luidt dat de Wbp van toepassing is op de verwerking van persoonsgegevens in het kader van activiteiten van een verantwoordelijke in Nederland.[27]

---

[23] J.M.A. Berkvens & J.E.J. Prins, *Recht en Praktijk: Privacyregulering in theorie en praktijk,* Deventer: Kluwer 2007, p.62.

[24] De juridische evaluatie: G. Overkleeft-Verburg, *De Wet persoonsregistratie. Norm, toepassing en evaluatie*, Zwolle 1995 en de sociaal-wetenschappelijke evaluatie: J.E.J. Prins e.a., *In het licht van de Wet persoonsregistratie: Zon, Maan of Ster?*, Alpen a/d Rijn 1995.

[25] 'Persoonsgegevens' Rijksoverheid, www.rijksoverheid.nl (zoek op 'persoonsgegevens'), geraadpleegd op 9 juni 2015.

[26] Artikel 2 Wbp.

[27] Artikel 4 Wbp.

Daarnaast is de Wbp van toepassing op de verwerking van persoonsgegevens door of ten behoeve van een verantwoordelijke die geen vestiging heeft in de Europese Unie, waarbij gebruik wordt gemaakt van al dan niet geautomatiseerde middelen die zich in Nederland bevinden. Tenzij deze middelen slechts worden gebruikt voor de doorvoer van persoonsgegevens. Tot slot wordt bepaald dat het de verantwoordelijke verboden is persoonsgegevens te verwerken, tenzij hij in Nederland een persoon of instantie aanwijst die namens hem handelt overeenkomstig de bepalingen van de Wbp.[28]

Naast de artikelen 2, 3 en 4 Wbp bepalen de begrippen 'persoonsgegeven' en 'verwerken' ook de reikwijdte van de Wbp.[29] De definitie van persoonsgegevens wordt nader uitgelegd in paragraaf 3.5.2. Met het oog op overeenkomsten behoeven gegevens niet primair betrekking te hebben op personen. Gedacht kan worden aan bijvoorbeeld: goederen, gebeurtenissen en gedachten. Indien daar sprake van is, en er persoonsgegevens mee gemoeid zijn, dienen zij blijkens de Memorie van Toelichting toch als persoonsgegevens te worden beschouwd.[30] Objectgegevens dienen echter in beginsel niet als een persoonsgegeven te worden beschouwd. Bestaat er desondanks een reële mogelijkheid dat er een verband, niet theoretisch, kan worden gelegd tussen het object en de persoon, dan is er waarschijnlijk wel sprake van een persoonsgegeven. Het objectgegeven valt dan wel onder de reikwijdte van de Wbp. [31] Het begrip verwerken is tevens opgenomen in de Wbp en heeft een zeer ruime strekking.[32] Voor de uitleg van het begrip 'verwerken' wordt daarom verwezen naar paragraaf 3.5.4. Concluderend beslaat de reikwijdte van de Wbp zich tot de verwerking van persoonsgegevens door verantwoordelijken die zich bevinden in Nederland. Voorts kan worden ingegaan op de rechtsbeginselen. Naast de reikwijdte, zijn rechtsbeginselen van belang voor de wetgeving. Rechtsbeginselen zijn immers de normen die aan geldende regels ten grondslag liggen.

[28] Artikel 4 Wbp.
[29] Kamerstukken II 1997/98, 25 892, nr. 3, p. 45-46 (MvT).
[30] Kamerstukken II 1997/98, 25 892, nr. 3, p. 46-47 (MvT).
[31] Kamerstukken II 1997/98, 25 892, nr. 3, p. 47 (MvT).
[32] Kamerstukken II 1997/98, 25 892, nr. 3. P, 50-53 (MvT).

3.4 Beginselen Wbp

Zoals beschreven in paragraaf 3.3 zijn rechtsbeginselen normen die aan geldende regels ten grondslag liggen. De rechtsbeginselen dienen daarom bij de rechtsvorming en rechtstoepassing in acht te worden genomen tijdens de overweging. Met andere woorden: rechtsbeginselen zijn richtinggevend bij de vorming en toepassing van het recht. De Wbp regelt onder welke voorwaarden persoonsgegevens mogen worden verwerkt en of de persoonsgegevens aan derden mogen worden verstrekt. Het uitgangspunt van de Wbp is dat de betrokkene, waar persoonsgegevens van worden verwerkt, zelf controle kan houden over zijn eigen persoonsgegevens. Het eerste beginsel van de Wbp is het transparantiebeginsel. Het transparantiebeginsel houdt in dat alleen de verantwoordelijke die de persoonsgegevens van de betrokkene verwerkt, aan de betrokkene meedeelt dat hij zijn gegevens verwerkt, voor welk doel en hoe lang hij de gegevens opslaat. Naast het transparantiebeginsel is het doelbindingsbeginsel ook opgenomen in de Wbp. Het doelbindingsbeginsel houdt in dat de gegevens alleen mogen verwerkt voor een van te voren welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doeleinde. Tot slot de beginselen proportionaliteit en subsidiariteit. Het proportionaliteitsbeginsel[33] houdt in dat de inbreuk op de belangen van de betrokkene niet onevenredig mag zijn in verhouding tot met het te dienen doel. Het subsidiariteitsbeginsel houdt in dat het doel waarvoor persoonsgegevens worden verwerkt in redelijkheid niet op een andere, voor de betrokkene, minder nadelige wijze kan worden bereikt.[34] Naast de normen vormen begrippen ook een belangrijk aspect van de Wbp. In de volgende paragraaf wordt daarom ingegaan op de begrippen.

[33] Het proportionaliteitsbeginsel wordt ook wel het evenredigheidsbeginsel genoemd.
[34] Mr. Dr. A.W. Duthler & Drs. A.J. Biesheuvel, *Het Europees privacyrecht in beweging*, Deventer: Kluwer 2013, p. 9-10.

3.5 Belangrijke begrippen

3.5.1 Inleiding

Begrippen zijn woorden die relaties uitdrukken en het daardoor mogelijk maken dat wat in taal wordt uitgedrukt te structureren.[35] Oftewel begrippen vormen de ruggengraat van de Wbp. Achtereenvolgens worden de belangrijkste begrippen in het kader van overeenkomsten zo volledig mogelijk uitgelegd.

3.5.2 Persoonsgegevens

Persoonsgegevens worden in de Wbp gedefinieerd als gegevens waarmee een natuurlijke persoon direct of indirect kan worden geïdentificeerd. Van direct identificerende gegevens is sprake wanneer gegevens betrekking hebben op een persoon waarvan de identiteit zonder veel omwegen eenduidig is vast te stellen. Voorbeelden van direct identificerende gegevens zijn NAW-gegevens, geboortedatum, geslacht etc. Daarnaast kunnen de gegevens niet direct tot identificatie van een persoon leiden maar via nadere stappen de gegevens in verband kunnen worden gebracht met een bepaalde persoon. Dit soort gegevens noemt men indirect identificerende gegevens. Die gegevens kunnen zijn ontdaan van de naam, echter onder omstandigheden door combinatie met andere gegevens weer worden teruggebracht tot een bepaalde persoon.[36]

3.5.3 Bijzondere gegevens

De Wbp kent voor de bijzondere gegevens een bijzonder aangescherpt regime. De verwerking van bijzondere gegevens is alleen toegestaan indien er sprake is van een zwaarwegend algemeen belang. Onder bijzondere gegevens kan worden verstaan iemands godsdienst, levensovertuiging, ras, politieke gezindheid, gezondheid en seksuele leven.[37] De Wbp geeft specifieke voorwaarden wanneer deze gegevens verwerkt mogen worden. Zo mogen gegevens betreffende iemands gezondheid worden verwerkt als dit gebeurt door hulpverleners, instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening.[38] Dit mag, voor zover dat met het oog op een goede behandeling of verzorging van de betrokkene, dan wel het beheer van de betreffende instelling of beroepspraktijk noodzakelijk is. De gegevens omtrent de gezondheid van iemand mogen alleen worden verwerkt door personen die vanwege ambt, beroep of wettelijk voorschrift of vanwege een overeenkomst tot geheimhouding zijn verplicht. In paragraaf 3.6 wordt nader aandacht besteed aan de verwerking van medische persoonsgegevens. Gegevens betreffende bijvoorbeeld iemands ras of etniciteit mogen alleen worden verwerkt als dit met het oog op de identificatie van de betrokkene en slechts voor dit doel onvermijdelijk is.

3.5.4 Verwerking

Van persoonsgegevens verwerking is al vrij snel sprake. Verwerken omvat namelijk elke handeling of elk geheel van handelingen ten aanzien van 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, evenals het afschermen, uitwissen of vernietigen van gegevens.[39]

3.5.5 De betrokkene

Degene op wie de persoonsgegevens betrekking hebben noemt men de betrokkene.[40] Dit is bijvoorbeeld de persoon van wie gegevens worden verwerkt met betrekking tot de gezondheid in een onderzoek. In de Wbp zijn bepalingen opgenomen die de betrokkene bepaalde rechten geven zoals: recht op inzage in zijn of haar gegevens[41], recht op het corrigeren van zijn of haar gegevens[42] en het recht om bezwaar te maken tegen de verwerking van de gegevens[43]. Het recht op inzage en op corrigeren van de gegevens komen tevens terug in artikel 10 lid 3 Grondwet en zijn daarom constitutioneel van aard.

[35] Definitie van het woord 'begrippen'
[36] Kamerstukken II 1997/98, 25 892, nr. 3, p. 48 (MvT).
[37] Artikel 16 Wbp.
[38] Artikel 21 Wbp.
[39] Artikel 1 onder b Wbp.
[40] Artikel 1 onder f Wbp.
[41] Artikel 35 Wbp.
[42] Artikel 36 Wbp.
[43] Artikel 40 Wbp.

3.5.6 De verantwoordelijke

De Wbp omschrijft 'de verantwoordelijke' als de natuurlijke persoon, de rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of tezamen met andere, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.[44] De verantwoordelijke is degene op wie, krachtens de Wbp, een aantal belangrijke verplichtingen rusten.[45] De voornaamste verplichting is dat de verantwoordelijke de doeleinden van de gegevensverwerking moet vaststellen, voor zover de wetgever dat niet zelf vaststelt omtrent de doeleinden van de gegevensverwerkingen. De Wbp richt zich dus primair tot de verantwoordelijke en bij iedere verwerking van persoonsgegevens kan er een verantwoordelijke worden aangemerkt.

De verantwoordelijke kan ook bestaan uit verschillende organen of uit verschillende natuurlijke personen als zij gezamenlijk het doel en de middelen voor de verwerking vaststellen. Bij meerdere personen kan bijvoorbeeld gedacht worden aan samenwerkingsverbanden waar verschillende natuurlijke personen en instellingen participeren in een gezamenlijk systeem. De verantwoordelijke in een samenwerkingsverband moet onderling worden overeengekomen. Meestal wordt gekeken naar wie bevoegd is om als verantwoordelijke op te treden. De verantwoordelijkheid kan dan ook in de volgende varianten worden opgesteld:

1. Er is één gemeenschappelijke verantwoordelijke die aansprakelijke is voor de verwerkingen als geheel, ondanks dat er verschillende organisaties deelnemen aan de verwerkingen. De andere deelnemende organisaties zijn alleen aansprakelijk voor de juistheid van de aangeleverde gegevens.
2. Er is geen sprake van een gemeenschappelijke verantwoordelijkheid, maar van afzonderlijke verantwoordelijkheid per (deel-)verwerking waar de verschillende verwerkingen min of meer zijn geïntegreerd. De betrokkene kan slecht één van de afzonderlijke verantwoordelijken aanspreken.
3. Er is sprake van een gemeenschappelijke verantwoordelijkheid waar verschillende verwerkingen zijn geïntegreerd zonder dat één gemeenschappelijke verantwoordelijke aanwezig is. Elk van de verantwoordelijken is aansprakelijk voor het geheel van de gegevensverwerkingen.[46]

Meestal wordt degene die het doel en de middelen van verwerking uitvoert aangemerkt als de verantwoordelijke. Het gaat daarbij met name om wie vaststelt of er überhaupt gegevens worden verwerkt, op welke wijze die gegevens worden verwerkt, welke bewerking wordt toegepast en tot slot voor welk doel. Er wordt in de Wbp dus met name gekeken naar de formeel juridische verantwoordelijke voor de gegevensverwerking, wat vaak ligt bij de rechtspersoon zelf. In een samenwerkingsverband is de meeste gerede partner vaak de verantwoordelijke. Dat is degene met de meeste bevoegdheden en de meeste betrokkenheid in een overleg. Desondanks is er soms toch sprake van een gezamenlijke verantwoordelijkheid.[47]

3.5.7 De bewerker

De Wbp omschrijft 'bewerker' als degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.[48] De verwerking van de gegevens ten behoeve van de verantwoordelijke wil zeggen overeenkomstig diens instructies en onder diens (uitdrukkelijke) verantwoordelijkheid. In dat geval is de bewerker niet aan het rechtstreekse gezag van de verantwoordelijke onderworpen.

De bewerker is een persoon of instelling die buiten de organisatie van de verantwoordelijk staat. Meestal betreft het een persoon of instelling die niet in een hiërarchische relatie staat ten opzichte van de verantwoordelijke. Is er wel sprake van een hiërarchische relatie met de verantwoordelijke, dan moet er worden gesproken van intern beheer. Als de verantwoordelijke gegevens buiten zijn rechtstreekse gezag verwerkt wil hebben, is de verantwoordelijke verplicht om een overeenkomst met een bewerker aan te gaan.[49] Het onderscheid tussen verantwoordelijke en bewerker is dus in de praktijk niet eenvoudig op te maken.

[44] Artikel 1 onder d Wbp.
[45] Artikel 15 Wbp.
[46] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 57-58 (MvT).
[47] CBP, *Informatie delen in samenwerkingsverbanden,* nummer 31A, februari 2012.
[48] Artikel 1 onder e Wbp.
[49] Artikel 14 lid 2 Wbp.

Voor de afbakening van het begrip bewerker is de relatie met de verantwoordelijke voor de gegevensverwerking en de wijze van zeggenschap waarmee de gegevensverwerking gepaard gaat bepalend.[50] De inhoud van de bewerkersovereenkomst is dus noodzakelijk en moet voldoen aan de wettelijke eisen die zijn gesteld in de Wbp.

De bewerkersovereenkomst[51] biedt de bewerker voldoende waarborging ten aanzien van de technische en organisatorische beveiligingsmaatregelen aangaande de verwerkingen die verricht moeten worden. De verantwoordelijke houdt altijd toezicht op de naleving van de technische en organisatorische beveiligingsmaatregelen. De bewerker kan ook alleen in opdracht van de verantwoordelijke gegevens verwerken. De persoonsgegevens die worden verwerkt in het kader van de overeenkomst moeten daarnaast voldoende beveiligd zijn. Tot slot moeten alle afspraken met de betrokkene in de bewerkersovereenkomst staan. De details van de verwerkingswijze kunnen aan de bewerker zelf worden overgelaten, zonder dat de bewerker daardoor verantwoordelijk of medeverantwoordelijke wordt. Het is echter wel zo dat de bewerker zich alleen beperkt tot het verwerken van de gegevens. De bewerker heeft dus geen zeggenschap over het doel van en de middelen voor de verwerkingen van persoonsgegevens. Als de bewerker namelijk wel zeggenschap heeft over het doel en de middelen voor de verwerkingen van persoonsgegevens, dan is er geen sprake meer van een bewerker, maar van een verantwoordelijke. Daar zit meteen de crux van het verhaal.[52]

Het begrip 'bewerker' moet beperkend worden geïnterpreteerd. Niet elke dienstverlener die optreedt namens de verantwoordelijke, is ook bewerker. Het bewerkersbegrip is in principe wel van toepassing op de verschillende vormen van dienstverlening, waarbij de dienstverlening betrekking heeft op het verwerken van persoonsgegevens. De beperkende interpretatie heeft betrekking op de gegevensverwerkingen die een uitvloeisel zijn van een andere vorm van dienstverlening. In dat geval is de dienstverlener wel zelf verantwoordelijk. Bijvoorbeeld: een arts die namens een cliënt optreedt is in beginsel zelf verantwoordelijk, omdat hij geacht wordt zeggenschap te hebben over de door hem bijgehouden cliëntgegevens.[53] Het bereik van het begrip wordt dus begrensd door enerzijds de interne beheerder die onder rechtstreeks gezag van de verantwoordelijke gegevens verwerkt en daarom geen bewerker is. En anderzijds het externe bureau dat zelfstandig in het kader van een opdracht van een rechtspersoon gegevens verwerkt en daarom zelf als verantwoordelijk kan worden aangemerkt.[54]

Alle belangrijk begrippen in het kader van overeenkomsten zijn nu aan de orde gekomen en duidelijk uitgelegd. In de volgende paragraaf wordt dieper ingegaan op de verwerking van medische persoonsgegevens, zoals aangegeven in paragraaf 3.5.3.

3.6 Verwerken van medische persoonsgegevens

Gezondheidsgegevens mogen alleen worden verwerkt door personen met een wettelijke geheimhoudingsplicht. Binnen het UMCG worden veel gegevens betreffende gezondheid verwerkt. Het verdient daarom de nodige aandacht om de wettelijke geheimhoudingsplicht te beschrijven. Het medisch beroepsgeheim is geregeld in verschillende wetgeving. Allereerst de Wet op de Beroepen in de Individuele Gezondheidszorg (in het vervolg Wet BIG). De Wet BIG bepaalt dat iedereen die een beroep uitoefent op het terrein van individuele gezondheidszorg verplicht is geheimhouding in acht te nemen ten opzichte van alles wat hem bij de uitoefening van zijn beroep op het gebied van de individuele gezondheidszorg als geheim is toevertrouwd, of waarvan hij als geheim kennis van heeft genomen, of waarvan hij kennis heeft genomen en hij moest begrijpen dat de informatie vertrouwelijk was.[55] Naast de Wet BIG, bepaalt de Wet op de Geneeskundige Behandelovereenkomst dat het medische dossier hooguit gegevens bevat die noodzakelijk zijn voor een goede hulpverlening, niet mag worden gedeeld met anderen. Het medische dossier mag alleen met de patiënt zelf en de

[50] Kamerstukken II 1997/98, 25 892, nr. 3, p.61 (MvT).
[51] Zie bijlage 4 voor de vereisten van een bewerkersovereenkomst.
[52] P.J. Hustinx, 'Begrip bewerker', *CBP,* 14 mei 2002 *(standpunt CBP over het begrip bewerker).*
[53] H.R. Kranenborg & L.F.M. Verhey, *Wet bescherming persoonsgegevens in Europees perspectief,* Deventer: Kluwer 2011.
[54] Kamerstukken II 1997/98, 25 892, nr. 3, p.62 (MvT).
[55] Artikel 88 Wet BIG.

hulpverleners die rechtstreeks bij de behandeling zijn betrokken worden gedeeld. Het uitwisselen van gegevens met anderen mag alleen met toestemming van de patiënt[56]. Desondanks wordt het medisch beroepsgeheim niet altijd goed nageleefd. Het College Bescherming Persoonsgegevens (in het vervolg CBP) heeft in 2013 een aantal zorginstellingen getoetst en kwam tot de conclusie dat bij slechts één van de zorginstellingen gedeeltelijk werd voldaan aan de wet.[57]

Tot slot dient het medische beroepsgeheim twee belangen. Allereerst het algemeen belang: iedereen moet zich vrijelijk tot een hulpverlener kunnen wenden, zonder vrees voor openbaarmaking van wat hij aan een hulpverlener zal toevertrouwen. En ten tweede het individuele belang: de patiënt moet erop kunnen vertrouwen dat zijn gegevens geheim worden gehouden en dat zijn privacy zal worden gerespecteerd.[58] Er zijn echter een aantal gronden geformuleerd waarop het beroepsgeheim wel mag worden doorbroken. Als er sprake van de volgende gronden is, mag het beroepsgeheim rechtsgeldig worden doorbroken:

- toestemming van de patiënt *of*
- informatie-uitwisseling met degenen die direct bij de behandeling zijn betrokken *of*
- wettelijk voorschrift *of*
- conflict van plichten *of*
- wetenschappelijk onderzoek.[59]

Achtereenvolgens zijn nu alle belangrijke aspecten m.b.t. overeenkomsten in de Wbp omschreven. Desondanks blijft er nu nog een vraag over en die heeft betrekking op toezicht en handhaving. Toezicht en handhaving wordt daarom kort uiteengezet in de volgende paragraaf.

[56] Artikel 7:457 BW.
[57] CBP, *Toegang tot digitale patiëntendossiers binnen zorginstellingen,* juni 2013 (onderzoeksrapport)
[58] V&VN Ambulancezorg, Ambulancezorg Nederland en Nederlandse Vereniging van Medische Managers Ambulancezorg, *Beroepsgeheim binnen de ambulancezorg; achtergrondnotitie en richtlijn.* Versie 2.0, augustus 2009.
[59] J.M.A. Berkvens, J.E.J. Prins, *Recht en Praktijk, Privacyregulering in theorie en praktijk*, Deventer: Kluwer 2007, p. 168-183.

3.7 Toezicht en handhaving

In de Wbp komen twee soorten toezichthouders aan de orde. Als extern toezichthouder: het CBP[60] en als interne toezichthouder: de functionaris voor de gegevensbescherming.[61] Het CBP is altijd bevoegd als toezichthouder, ongeacht of er een functionaris voor de gegevensbescherming binnen een organisatie is aangesteld. Daarnaast is het CBP als toezichthouder ook belast met de handhavingsbevoegdheid. De functionaris voor de gegevensbescherming heeft die bevoegdheid niet op grond van de Wbp.

Het CBP is een organisatie die zich niet alleen strekt tot de Wbp, maar strekt zich ook uit tot andere wetten, algemene maatregelen van bestuur en andere wettelijke regelingen op grond waarvan persoonsgegevens worden verwerkt. De functionaris voor de gegevensbescherming strekt zich daarentegen wel alleen uit tot de Wbp. De functionaris voor de gegevensbescherming heeft als taak het toezicht houden op de verwerking van persoonsgegevens door een verantwoordelijke. Meestal benoemd een verantwoordelijke of een organisatie waarbij verantwoordelijken zijn aangesloten zelf een eigen functionaris voor de gegevensbescherming. Het is echter niet verplicht om een functionaris voor de gegevensbescherming te benoemen, dit blijkt uit het woord 'kan'.[62]

3.8 Conclusie

De belangrijkste materie voor de beantwoording van de eerste theoretische deelvraag is aan bod gekomen. De Wbp wordt grotendeels ingetrokken als de EPV geïmplementeerd moet worden in de Nederlandse wetgeving. Desondanks komen veel aspecten uit de Wbp mogelijk terug in de EPV. Met name ten aanzien van de begrippen en beginselen vormt de Wbp een goed kader om verder op te borduren. In het volgende hoofdstuk wordt hier verder op ingegaan en zal waar nodig worden verwezen naar hoofdstuk 3.

[60] Artikelen 51-61 Wbp.
[61] Artikelen 62-64 Wbp.
[62] Artikel 62 Wbp.

4 EUROPESE PRIVACY VERORDENING

4.1 INLEIDING

De Wbp is grotendeels in hoofdstuk 3 uiteengezet met het oog op overeenkomsten. Door deze uiteenzetting kan verder worden gegaan met hoofdstuk 4. In hoofdstuk 4 worden antwoorden geformuleerd op de tweede, derde en vierde theoretische deelvragen. De deelvragen luiden:

- *Wat is vastgelegd in de nieuwe Europese Privacy Verordening met betrekking tot contracten?*
- *Waar dient een compliant contract met als uitgangspunt de Europese Privacy Verordening aan te voldoen?*
- *Wat wordt gesteld belangrijk te zijn uit de (juridische) literatuur omtrent de gevolgen van de Europese Privacy Verordening?*

Achtereenvolgens worden de volgende onderwerpen besproken: geschiedenis (§ 4.2), reikwijdte (§ 4.3), beginselen EPV (§ 3.4), belangrijke begrippen (§ 4.5), vereisten contracten tussen verantwoordelijken (§ 4.6), vereisten contracten verwerker (§ 4.7), privacy en security by design en by default (§ 4.8), meldplicht datalekken (§ 4.9), toezicht en handhaving (§ 4.10) en tot slot een conclusie § 4.11). Door deze theoretische uiteenzetting worden op het einde de onderzoekspunten geformuleerd (§ 4.12).

4.2 GESCHIEDENIS

De Europese Unie wil de privacy van de verwerking van persoonsgegevens beter beschermen door de invoering van de EPV. De Europese Unie wil de privacy van gegevensverwerking beter beschermen, gezien de huidige omvang van gegevensverwerking binnen de Europese Unie. De geldende Europese en nationale wetgevingen sluiten namelijk niet voldoende aan op de nieuwe technologieën waar informatie mee wordt verzameld. De Europese Commissie kwam daarom in januari 2012 met het voorstel voor een nieuwe verordening om de 'privacy' van eenieder in de Europese Unie beter te waarborgen. De EPV wordt gezien als het meest geschikte rechtsinstrument, gezien deze rechtstreeks toepasbaar is binnen de lidstaten. Hierdoor is de juridische fragmentatie minder en wordt de rechtszeker heid gestimuleerd. De doelstelling en beginselen van de huidige Richtlijn 95/46/EG en de Wbp gelden nog steeds, zo blijkt uit de toelichting van de Europese Commissie.[63] Nederland is in zijn algemeenheid positief over het voorstel voor de EPV. Het is namelijk van mening dat de huidige EU-privacyrichtlijn te kort schiet om een niveau van gegevensbescherming te garanderen, dat voldoende aansluit bij de behoeften van burgers en bedrijven. In dit hoofdstuk wordt uitgegaan van de tekst van de EPV, zoals die door de Europese Commissie bij het Europees Parlement en de Raad is ingediend. Het Europees Parlement heeft op 12 maart 2014 een wetresolutie betreffende 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 gehouden.
De wettekst van de EPV is dus nog in ontwikkeling, maar op hoofdlijnen staat het vast. In bijlage 3 is een beknopt, maar duidelijk overzicht opgenomen van de veranderingen en de gevolgen die de EPV met zich meebreng. Door deze korte uiteenzetting van de geschiedenis kan vervolgens worden ingegaan op de reikwijdte van de EPV.

4.3 REIKWIJDTE

De reikwijdte van de EPV wordt bepaald door de artikelen 2 en 3 EPV. De materiële reikwijdte bepaalt dat de verordening van toepassing is op geheel of gedeeltelijk geautomatiseerde verwerkingen van persoonsgegevens, alsmede op de niet-geautomatiseerde verwerkingen van persoonsgegevens die in een bestand zijn opgenomen, of bestemd zijn om daarin te worden opgenomen.[64] De EPV wordt in vergelijking met de Wbp uitgebreid ten aanzien van het geografisch toepassingsgebied. De geografische reikwijdte beslaat namelijk het grondgebied van de Unie en daarnaast is de verordening van toepassing op de 'niet' in de Unie gevestigde verantwoordelijke.[65] Dit laatste betekent: dat als de

[63] Verordening (EU) 0011/2012.
[64] Artikel 2 van de voorgestelde Europese Privacy Verordening.
[65] Artikel 3 van de voorgestelde Europese Privacy Verordening.

verantwoordelijke verwerkingen verricht die betrekking hebben op het aanbieden van goederen en/of diensten binnen de Unie, de verantwoordelijke onder de werkingssfeer van de EPV valt. Bijvoorbeeld: een betrokkene in Nederland koopt online iets in China. In dat geval betekent dat de verwerking van persoonsgegevens die daarvoor nodig zijn worden beheerst door de verordening.[66] Naast de artikelen 2 en 3 EPV bepalen de begrippen 'persoonsgegeven' en 'verwerken' ook de reikwijdte van de EPV. Deze begrippen worden uitgelegd in paragraaf 4.5.2 en paragraaf 4.5.4. Concluderend beslaat de reikwijdte van de EPV zich tot verwerking van persoonsgegevens door een verantwoordelijke die zich bevindt in de Europese Unie en daarnaast is de verordening van toepassing op de 'niet' in de Unie gevestigde verantwoordelijke. Kortom, de EPV heeft de geografische reikwijdte in vergelijking met de Wbp drastisch aangepast. Naast de reikwijdte zijn rechtsbeginselen ook van belang voor de verordening. Immers in paragraaf 3.4 werd al aangegeven dat rechtsbeginselen de normen zijn die aan geldende regels ten grondslag liggen.

4.4 Beginselen EPV

Zoals besproken in paragraaf 3.4 zijn rechtsbeginselen richtinggevend bij de vorming en toepassing van het recht. De algemene beginselen, zoals omschreven in paragraaf 3.4, die aan elke verwerking van persoonsgegevens ten grondslag behoren te liggen, zijn wederom van toepassing op de EPV. Er zijn echter wat accentverschillen te zien. Aan de algemene beginselen worden twee belangrijke elementen toegevoegd. Het transparantiebeginsel wordt nu uitdrukkelijk geformuleerd in de EPV. Wat kortgezegd betekent dat het vermijden van geheimzinnige activiteiten bij alle aspecten van de verwerking van persoonsgegevens moet worden verwezenlijkt. Een nieuw beginsel, dat is geformuleerd, is de verantwoordingsplicht van de verantwoordelijke. Wie als verantwoordelijke persoonsgegevens verwerkt is verplicht dat openlijk te doen en over de aard en doel van die verwerking aan de betrokkene en de toezichthouder zelf verantwoording af te leggen. Dit beginsel is van belang, gezien de toezichthouder niet meer kan nagaan welke verwerkingen door een verantwoordelijke worden verricht. De betrokkene en de toezichthouder die inzicht willen in de verwerkingen dienen daar nu voor bij de verantwoordelijk te zijn. [67] Vervolgens worden in paragraaf 4.4 de begrippen die van belang zijn in het kader van overeenkomsten besproken.

4.5 Belangrijke begrippen

4.5.1 Inleiding

In paragraaf 3.4.1 werd al aangegeven dat begrippen de ruggengraat vormt van wetgeving. De EPV introduceert een aantal nieuwe begrippen, maar heeft ook een aantal begrippen van naam gewijzigd.[68] In deze paragraaf worden de belangrijkste begrippen uiteengezet. Sommige begrippen zijn hetzelfde gebleven ten aanzien van de Wbp, indien niet letterlijk verwoord dan toch qua strekking. Waar de begrippen hetzelfde zijn gebleven is gekozen voor een beknopte beschrijving, waarbij wordt verwezen naar een uitgebreidere uitleg in paragraaf 3.5.

4.5.2 Persoonsgegevens

Persoonsgegevens[69] worden gedefinieerd als iedere informatie betreffende een betrokkene.[70]

4.5.3 Bijzondere gegevens

De EPV kent net als de Wbp voor de bijzondere gegevens een aangescherpt regime. De verwerking van bijzondere gegevens is in eerste instantie streng verboden, tenzij er sprake is van een zwaarwegend algemeen belang.[71] Onder bijzondere gegevens kan worden verstaan iemands godsdienst, levensovertuiging, ras, politieke gezindheid, ge-

[66] J.P. de Jong, Regelmaat, *De Algemene verordening gegevensbescherming. De rechtsopvolger van de Wbp,* Boom Juridische Uitgever: 2015, p.9.

[67] J.P. de Jong, Regelmaat, *De Algemene verordening gegevensbescherming. De rechtsopvolger van de Wbp,* Boom Juridische Uitgever: 2015, p.9-10.

[68] Artikel 4 van de voorgestelde Europese Privacy Verordening.

[69] Zie hier het begrip ' persoonsgegevens' in § 3.5.2 voor een uitgebreidere uitleg.

[70] Artikel 4 onder 2 van de voorgestelde Europese Privacy Verordening.

[71] Artikel 9 lid 2 van de voorgestelde Europese Privacy Verordening.

zondheid en seksuele leven.[72]

4.5.4 Verwerking

De definitie van verwerking is vergelijkbaar met die van de Wbp: namelijk elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enigerlei andere wijze van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het wissen of vernietigen van gegevens.[73]

4.5.5 De betrokkene

De betrokkene is degene waar de persoonsgegevens van worden verwerkt. De betrokkene is een geïdentificeerde natuurlijke persoon of een natuurlijke persoon die direct of indirect kan worden geïdentificeerd. De identificatie vindt plaats aan de hand van een identificatienummer, gegevens over de verblijfplaats, een online-identificatiemiddel of één of meer specifieke elementen die kenmerkend zijn voor zijn fysieke, fysiologische, genetische, mentale, economische, culturele of sociale identiteit.[74]

De rechten van de betrokkene veranderen op grond van de EPV ingrijpend. Het recht op toegang,[75] rectificatie,[76] wissen en afscherming van gegevens[77] worden nu allemaal apart beschreven. Inhoudelijk veranderen de rechten op toegang en rectificatie niet, alsook het recht op bezwaar blijft bestaan.[78] Het recht op wissen en afscherming van gegevens gaat wel ingrijpend veranderen. Het recht op het wissen van gegevens is namelijk een nieuw recht onder de EPV. Als gegevens gelet op het doel van de verwerking niet langer meer nodig zijn, dan heeft de betrokkene recht op het wissen van zijn gegevens.[79] Dit geldt ook als de betrokkene de verleende toestemming intrekt, het recht op verzet uitoefent of wanneer de gegevens in strijd met de EPV zijn verwerkt.

4.5.6 De verantwoordelijke

De definitie van de verantwoordelijke is grotendeels hetzelfde gebleven.[80] De verantwoordelijke is namelijk een natuurlijke of rechtspersoon, de overheidsinstantie of enig ander orgaan die, respectievelijk dat, alleen of tezamen met anderen het doel van en de voorwaarden en middelen voor de verwerking van persoonsgegevens vaststelt.[81] Wederom kan de verantwoordelijke ook bestaan uit verschillende organen of uit verschillende natuurlijke personen als zij gezamenlijk het doel en de middelen voor de verwerking vaststellen.[82] In de EPV krijgt de verantwoordelijke ook een nieuwe verplichting: de meldplicht datalekken. De meldplicht datalekken wordt verder uitgelegd in paragraaf 4.7.

4.5.7 De verwerker

De Wbp spreekt van 'bewerker' en de EPV van 'verwerker'. De terminologie is anders, maar betekent in feite hetzelfde.[83] De verwerker is 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.[84]

4.6 Vereisten contracten tussen verantwoordelijken

De EPV geeft geen specifieke eisen aan overeenkomsten met andere verantwoordelijken, behalve als het gaat om

[72] Artikel 9 van de voorgestelde Europese Privacy Verordening.
[73] Artikel 4 onder 3 van de voorgestelde Europese Privacy Verordening.
[74] Artikel 4 onder 1 van de voorgestelde Europese Privacy Verordening.
[75] Artikel 15 van de voorgestelde Europese Privacy Verordening.
[76] Artikel 16 van de voorgestelde Europese Privacy Verordening.
[77] Artikel 17 van de voorgestelde Europese Privacy Verordening.
[78] Artikel 19 van de voorgestelde Europese Privacy Verordening.
[79] Artikel 17 van de voorgestelde Europese Privacy Verordening.
[80] Zie hier het begrip ' de verantwoordelijk' in § 3.5.6 voor een uitgebreidere uitleg.
[81] Artikel 4 onder 5 van de voorgestelde Europese Privacy Verordening.
[82] Artikel 24 van de voorgestelde Europese Privacy Verordening.
[83] Zie hier het begrip ' de bewerker' in § 3.5.7 voor een uitgebreidere uitleg.
[84] Artikel 4 onder 6 van de voorgestelde Europese Privacy Verordening.

bijvoorbeeld een samenwerkingsverband. Als er wordt samengewerkt en in het kader daarvan de doelen en middelen voor de samenwerking van persoonsgegevens gezamenlijk worden vastgesteld, moet er onderling een regeling vastgesteld worden.[85] Hierbij kan gedacht worden aan een samenwerkingsovereenkomst of convenant waarin ieders verantwoordelijkheden worden vastgesteld. Van belang is dat met name ten aanzien van de betrekking tot de procedures en mechanismen voor de uitoefening van de rechten van de betrokkene worden opgenomen in de overeenkomst. Er moet hierbij worden weergegeven wat ieders rol in de gezamenlijke verwerking is en wat hun verhouding is tot de betrokkene. De wezenlijke inhoud hiervan moet aan de betrokkene kenbaar worden gemaakt. Als de inhoud niet kenbaar/ duidelijk is met betrekking tot de inhoud van de verantwoordelijkheid, zijn alle voor de verwerking verantwoordelijken hoofdelijk aansprakelijk.

4.6.1 Reikwijdte verantwoordelijkheid UMCG bij verwerker

De EPV bepaalt dat een organisatie als verantwoordelijke alleen verantwoordelijk is voor de gegevens die de verwerker in opdracht van de organisatie verwerkt, dus volgens de instructies van de organisatie.[86] De organisatie is niet meer verantwoordelijk voor andere gegevensverwerkingen die bij de verwerker plaatsvinden. In dit laatste geval dienen er wel afspraken worden gemaakt over de uitoefening van de rechten van de betrokkene.[87]

4.7 Vereisten contracten verwerker

Wanneer er namens een verantwoordelijke persoonsgegevens worden verwerkt, moet de verantwoordelijke een verwerker benaderen die voldoende waarborging biedt ten aanzien van de tenuitvoerlegging van passende technische en organisatorische maatregelen en procedures. Dit moet geschieden op een dusdanige wijze dat de verwerking voldoet aan de vereisten van de EPV en daarnaast dat de rechten van de betrokkene worden beschermd. Deze activiteiten moeten door de verwerker worden geregeld door een overeenkomst of door een andere rechtshandeling die de verwerker ten opzichte van de verantwoordelijke bindt. De EPV somt in artikel 26 een aantal vereisten voor een verwerkersovereenkomst op. Hieronder staat een opsomming van de vereisten voor een verwerkersovereenkomst. In bijlage 4 is een overzicht opgenomen met de vereisten die gelden voor een verwerkersovereenkomst en een bewerkersovereenkomst. Dit om de verschillen aan te kunnen tonen. Hieruit blijkt dat de EPV nu meer en strengere eisen stelt aan de overeenkomst ten opzichte van de bewerkersovereenkomst uit de Wbp.

Vereisten voor een verwerkersovereenkomst:

1. Verwerking kan slechts in opdracht van de verantwoordelijk.
2. Afspraken omtrent verzoeken van betrokkenen dienen te worden opgenomen.
3. Persoonsgegevens zijn voldoende beveiligd. (bijv. NEN7510)[88]
4. De verwerker biedt voldoende waarborging ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de verwerkingen.
5. De verantwoordelijke ziet toe op de naleving van de technische en organisatorische beveiligingsmaatregelen.
6. De verwerker moet de beveiliging aantonen m.b.v. gedragscodes of certificeringsmechanismen.
7. Meldplicht van datalekken aan de verantwoordelijke.
8. Geheimhouding/ vertrouwelijkheid.
9. Na beëindigen van de overeenkomst moet de verwerker alle resultaten teruggeven en kopieën verwijderen.
10. De verwerker mag niet zonder toestemming een andere verwerker in dienst nemen, tenzij anders is overeengekomen tussen partijen.

4.8 Privacy en security by design en by default

Zoals opgenomen in paragraaf 1.1.1 brengt de EPV gevolgen met zich mee. Een aantal gevolgen zijn al aan de orde gekomen in dit hoofdstuk, zoals de uitgebreidere rechten

[85] Artikel 24 van de voorgestelde Europese Privacy Verordening.
[86] Artikel 26 lid 4 van de voorgestelde Europese Privacy Verordening.
[87] Artikel 24 van de voorgestelde Europese Privacy Verordening.
[88] De norm NEN 7510 is een door het Nederlands Normalisatie-instituut ontwikkelde norm voor Informatiebeveiliging voor de zorgsector in Nederland.

van betrokkenen. Voor hoofdstuk 6 is het van belang dat het gevolg 'privacy en security by design en by default' kort wordt uitgelegd. Privacy en security by design en by default betekent dat de organisatie de privacyaspecten moet meewegen bij het ontwikkelen van nieuwe producten en diensten.[89] Met andere woorden: privacy is relevant voor de ontwikkeling van producten en diensten. Allereerst zal er worden ingegaan op het begrip privacy by design. Privacy by design gaat over het ontwerpen van informatiesystemen, die de privacy van mensen beschermen: door gegevensminimalisatie; door transparantie over het gebruik van hun gegevens; door afscherming van de identiteit van het individu; door het gebruik van kleefbeleid[90]; door het volgen van persoonsgegevens nadat deze zijn verzameld; door het gebruik van privacy bewustmakende icons en door privacy ontologie waardoor de privacyrechtsregels in systemen zijn in te bouwen.[91] Privacy by default lijkt op het vorige begrip en betekent dat door middel van systeeminstellingen maximale privacy van een betrokkene worden gewaarborgd en voor zover mogelijk door het systeem wordt afgedwongen.[92] Kortom, privacy en security by design en by default is een belangrijk aspect in het kader van compliance. In de volgende paragraaf wordt het gevolg 'meldplicht datalekken' beschreven. De uiteenzetting van dit gevolg is van belang voor de verantwoordelijke.

4.9 Meldplicht datalekken

In de EPV is een meldplicht datalekken opgenomen, een verplichting van de verantwoordelijke. Ingeval van een datalek, als bijvoorbeeld een laptop van een arts wordt gestolen met medische informatie, is de verantwoordelijke verplicht zonder onnodige vertraging en zo mogelijk niet later dan 24 uur nadat hij ervan kennis heeft genomen deze datalek te melden bij het CBP en de betrokkene.[93] De verwerker is verplicht de verantwoordelijke onmiddellijk te waarschuwen en te informeren na vaststelling van de datalek. De melding door de verantwoordelijk aan het CBP omvat tenminste:

- een omschrijving van de aard van de inbreuk;
- de vermelding van de identiteit en contactgegevens van de functionaris voor de gegevensbescherming of ander contactpunt;
- aanbevelingen voor maatregelen om nadelige gevolgen te verminderen;
- een omschrijving van de gevolgen van de inbreuk;
- een omschrijving van de maatregelen die de verantwoordelijke heeft voorgesteld of genomen om de inbreuk aan te pakken.[94]

Vervolgens kan het onderwerp toezicht en handhaving worden uitgelegd. Na paragraaf 4.10 volgt nog een korte uiteenzetting van de sancties bij niet-naleving van de EPV.

4.10 Toezicht en handhaving

Uit de verordening blijkt dat er een omvangrijke regeling voor de onderlinge samenwerking tussen de toezichthouders van de 28 lidstaten van de Europese Unie is gesteld. Het is echter zo dat bij een verordening zoals de EPV er een centrale EU toezichthouder past. Dit, omdat de regels uniform moeten worden uitgelegd. Dit laatste is echter niet te bewerkstelligen, gezien de aard van het gegevensbeschermingsrecht. Dit maakt het daarom onmogelijk om een toezichthouder in de Europese Unie aan te stellen. Een EU toezichthouder zou dan 500 miljoen burgers moeten bedienen, wat een onmogelijk taak is. De nationale toezichthouders van de lidstaten blijven daarom onmisbaar, zoals het CBP in Nederland.[95] Een organisatie moet nu echter wel verplicht een functionaris voor de gegevensbescherming

---

[89] A.W. Duthler & A.J. Biesheuvel, *Het Europese privacyrecht in beweging,* Deventer: Uitgeverij Kluwer 2013, p. 27.

[90] Door middel van cryptografische technieken kunnen privacy voorkeuren aan gegevens worden 'geplakt' , zodat organisaties niet afwijken van de aan de websitebezoeker toegezegde manier van gegevensverwerking.

[91] J. Borking, '*Privacy by design en 'data protection by default'.* n: Privacy en Compliance – 03-04/2012, p. 6.

[92] J. Borking, '*Privacy by design en 'data protection by default'.* n: Privacy en Compliance – 03-04/2012, p. 9.

[93] Artikel 31 jo 32 van de voorgestelde Europese Privacy Verordening.

[94] A.W. Duthler & A.J. Biesheuvel, *Het Europese privacyrecht in beweging,* Deventer: Uitgeverij Kluwer 2013, p. 25.

[95] J.P. de Jong, Regelmaat, *De Algemene verordening gegevensbescherming. De rechtsopvolger van de Wbp,* Boom Juridische Uitgever: 2015, p. 13.

aanstellen.[96] De verplichte aanstelling binnen het UMCG moet plaatsvinden, gezien het UMCG een organisatie is met meer dan 250 medewerkers.[97] Als er geconstateerd wordt door een toezichthouder dat de EPV niet wordt nageleefd, kan er een sanctie volgen. Deze sancties zijn uiteengezet in de volgende paragraaf.

4.11 Gevolgen niet-naleving EPV

De EPV kent een sluitend stelsel van administratieve sancties. Er kan worden gesproken van bestuurlijke boetes bij niet-naleving van de EPV. De boetes die kunnen worden gegeven zijn niet mis en ontzettend hoog. De diverse categorieën stellen bij niet-naleving van de EPV dat:

1. de toezichthoudende autoriteit een geldboete oplegt tot € 250.000,- of, bij een onderneming, een geldboete van 0,5 % van de jaarlijkse wereldwijde omzet op concernniveau;
2. de toezichthoudende autoriteit een geldboete oplegt tot € 500.000,- of, bij een onderneming, een geldboete van 1 % van de jaarlijkse wereldwijde omzet op concernniveau;
3. de toezichthoudende autoriteit een geldboete oplegt tot € 1,000000,- of, bij een onderneming, een geldboete van 2 % van de jaarlijkse wereldwijde omzet op concernniveau. [98]

4.12 Conclusie

Als er wordt gekeken naar de inhoud van de EPV is er op het gebied van de materiële regels sprake van een combinatie van continuïteit en verandering. Het geldend recht keert veelal terug in de verordening, echter worden de rechten van de betrokkenen en de verplichtingen van de verantwoordelijke verder uitgebreid. In het kader van overeenkomsten worden er meerdere en strengere eisen gesteld. Het toezicht op naleving en de sanctionering van de EPV zijn niet te vergelijken met de geldende wet- en regelgeving binnen de Europese Unie en Nederland. De sanctionering in de EPV is namelijk schrikbarend hoog. Met andere woorden: de EPV vraagt meer aantoonbaarheid, in vergelijking met de Wbp, van een organisatie met betrekking tot het overzicht en inzicht van gegevensverwerking. Ten aanzien van gegevensverwerkingen in contracten kan een organisatie inzicht en overzicht aantonen door middel van een goed functionerend contractbeheer. Hier gaat het volgende hoofdstuk over.

4.13 Onderzoekspunten

De onderzoekspunten uit dit hoofdstuk zijn:

- *Is het UMCG op dit moment EPV-compliant?*
- *Voldoen de standaardcontracten van het UMCG aan de EPV?*

[96] Artikel 35 van de voorgestelde Europese Privacy Verordening.
[97] Artikel 35 lid 2 sub b van de voorgestelde Europese Privacy Verordening.
[98] Artikel 79 van de voorgestelde Europese Privacy Verordening.

5 Contractbeheer

5.1 Inleiding

De relevante wetgevingen zijn nu besproken, waardoor nu kan worden overgaan op het onderwerp contractbeheer. Contractbeheer kan namelijk worden gezien als een instrument om inzicht en overzicht te krijgen in contracten binnen een organisatie. Inzicht en overzicht van de gegevensverwerking is immers een vereiste van de EPV. Dit hoofdstuk is daarom van belang en zal een antwoord worden geven op de vijfde theoretische deelvraag. Deelvraag vijf luidt:

- *Wat is bekend in de literatuur over contractbeheer?*

Achtereenvolgens worden de volgende onderwerpen besproken: contractbeheer (§ 5.2), het contractbeheerproces (§ 5.3), organisatie van het contractbeheerproces (§ 5.4) en tot slot zal worden afgerond met een conclusie (§ 5.4) en volgen de onderzoekspunten (§ 5.5).

5.2 Contractbeheer

Contractbeheer wordt gedefinieerd als het proces dat ervoor zorgt dat de juiste informatie op het juiste tijdstip op de juiste plaats is, ter ondersteuning van het gehele contracteringsproces. Dit betekent kortgezegd dat de informatie kan bestaan uit het contract zelf, maar ook uit informatie van het contract of informatie over het contract. Het contracteringsproces heeft betrekking op het moment waarop het initiatief ontstaat tot het sluiten van een contract tot en met het beëindigen van een contract en daarnaast de eventuele nazorg. Het doel van contractbeheer is om de interne organisatie voldoende inzicht te verschaffen in (lopende) contracten en daarnaast de juiste contractuele afspraken en informatie verkrijgen door het voeren van een daarvoor bestemde administratie. Om een goed contractbeheer te bewerkstelligen is het noodzakelijk dat de informatie altijd up-to-date is en beschikbaar voor de betrokkenen en bevoegden.[99]

Uit voornoemde luiden daarom de volgende doelstellingen van contractbeheer:

1. Brengt discipline in de zorg voor ondertekening en bewaring van de ondertekende contracten.
2. Levert een mogelijkheid tot het bewaken van de opgenomen termijnen voor opzegging, betaling, verlening, evaluatie enz.
3. Geeft een overzicht van contractuele verplichtingen jegens de verschillende wederpartijen.
4. Bij verkoopcontracten levert het inzicht op in de vraag bij hoeveel verkoopcontracten de algemene voorwaarden van toepassing zijn, welke kortingspercentages zijn verleend of andere bijzondere verkoopvoorwaarden.
5. Bij inkoopcontracten geeft het een mogelijkheid tot het inventariseren van bepaalde rechten, zoals volumes, prijzen en verplichtingen.
6. Biedt een systeem voor het bijhouden van metainformatie: wie is verantwoordelijk voor het contract, waar is het originele contract fysiek en wie is de contactpersoon voor het contact bij de wederpartij.
7. Het functioneren als aanzet om te komen tot een benchmark van de verschillende contracten, die voor gelijksoortige producten of dienstverlening zijn gesloten tot een benchmark van contractuele voorwaarden.
8. Voor het beëindigen van contracten; op een voor de organisatie zo gunstig mogelijk moment. [100]

Beheersmatig betekent dit:

1. (De)centraal beschikbaarheid van informatie uit contracten.
2. Totstandkoming van contracten door de juiste personen (verantwoordelijke) in de organisatie op het juiste moment.
3. Bewaking en rapportage van de in de contacten vastgelegd activiteiten op het juiste moment door de juiste persoon (verantwoordelijke).

[99] V.S.M. Hijl, D. Van der Meer, *Contractbeheer, Theorie in praktijk*, Heerde: Mercante Publishing, 2002, p. 15-22.

[100] B.H.A. van Leeuwen, A.G.H. van der Staay & O. Javornik, *beroep: Bedrijfsjurist, Praktische leidraad voor bedrijfsjuristen*, Deventer: Kluwer, 2009, p. 198-199.

Door het voeren van een overzichtelijk contractbeheer wordt er een beheersbare situatie gecreëerd. Door het ontbreken van een centraal inzicht in de geldende contracten ontstaat er logischerwijze een onbeheersbare situatie. De onbeheersbare situatie heeft tot gevolg dat contracten zoek raken, oude contracten blijven in stand en zwerven door de organisatie heen, informatie uit geldende contracten blijven onbenut en contracten worden niet op tijd verlengd of beëindigd. Een disfunctionerend contractbeheer heeft daarom (grote) financiële consequenties ten gevolge.[101]

5.3 Het contactbeheerproces

Het contracteerproces kan op de volgende wijze worden beschreven:
- sluiten van contracten (specifiëren, selecteren en contracteren);
- registratie van de contracten (contractbeheer);
- managen van de uitputting en mutatie bij wijzigingen van contracten (management van contracten);
- bewaken van de contracten (verlengen en beëindigen).

5.3.1 Fase 1: Specifiëren van de behoefte

Het contractbeheerproces begint met het sluiten van een contract, er ontstaat een behoefte tot contracteren. Als deze behoefte onderkend is, moet die behoefte nader worden gespecificeerd. Daarnaast wordt in deze eerste fase globaal de te verrichten tegenprestaties gedefinieerd.

In de eerste fase wordt er gestreefd naar effectiviteit en uitvoerbaarheid van het contracteren. De effectiviteit wordt gedefinieerd als de mate waarin de overeengekomen te ontvangen prestatie in een behoefte voorziet. Om een goed en effectief contract op te stellen is het nodig om die behoefte te kennen. Voornoemde kan worden gerealiseerd door het inzamelen van informatie door degenen (de gebruiker) bij wie de behoefte tot contracteren ontstaat. Informatie kan zijn; een beschrijving van in te kopen goederen, verwachte activiteiten van de wederpartij bij een samenwerkingscontract etc. Naast de effectiviteit is uitvoerbaarheid ook een belangrijk begrip in de eerste fase. De uitvoerbaarheid heeft betrekking op hoe de overeengekomen te leveren prestatie kan worden gerealiseerd. Er moet dus bekeken worden of er aan de te leveren prestaties kan worden voldaan. Uiteindelijk rolt er in de eerste fase een specificatiedocument uit op basis van de informatie verkregen uit de effectiviteit en uitvoerbaarheid.[102]

5.3.2 Fase 2: Selecteren van de wederpartij

Als de behoefte voldoende gespecificeerd is in de eerste fase volgt er een marktoriëntatie om te komen tot een geschikte contractpartner. Op basis van de volgende activiteiten kan een geschikte contractpartner worden gevonden. Het is niet noodzakelijk dat alle activiteiten worden volbracht. Het uitgangspunt bij het selecteren is immers de kwaliteitseis van voordeligheid.[103] De kwaliteitseis van voordeligheid staat voor de verhouding tussen de waarden van de te ontvangen en de te leveren prestatie.
- Opstellen van eisenpakket.
- Voorselectie van wederpartijen.
- Voorbereiding en aanvraag van reacties.
- Selectie uit de reacties.
- Onderhandelingen.
- Definitieve contractpartner keuze.[104]

5.3.3 Fase 3: Opstellen en tekenen van het contract

Als de contractpartij is gekozen door de organisatie, moet er een duidelijk contract worden opgesteld. Bij het opgestelde contract moeten de algemene voorwaarden ook worden opgenomen, omdat in de algemene voorwaarden onderwerpen worden vastgelegd die niet in het contract zelf staan. Tijdens het opstellen/ beoordelen van het contract dienen de volgende kwaliteitseisen in acht te worden genomen: volledigheid, duidelijkheid en legaliteit. Om het contract volledig te maken is het noodzakelijk om de prestatie goed te omschrijven en daarnaast worden de volgende punten opgenomen:

[101] Publicatie NPPP, *Contractbeheer en contractmanagement*, juni 2004.

[102] V.S.M. Hijl, D. Van der Meer, *Contractbeheer, Theorie in praktijk*, Heerde: Mercante Publishing, 2002, p. 39-40.

[103] T. Knoester, *Management in de praktijk,* Houten: Bohn Stafleu van Loghum, 2005, p.23.

[104] V.S.M. Hijl, D. Van der Meer, *Contractbeheer, Theorie in praktijk*, Heerde: Mercante Publishing, 2002, p. 40-42.

- considerans en doelomschrijving;
- welke prestatie wordt geleverd;
- leveringscondities;
- waar wordt de prestatie geleverd;
- wanneer wordt de prestatie geleverd;
- algemene voorwaarden;
- eigendomsoverdracht;
- bankgaranties;
- boete- en/of premieregeling;
- garantiebepalingen;
- geschillenregelingen;
- geldigheidsduur en opzegtermijn;
- ontbindingsgevolgen;
- resterende contractuele afspraken.[105]

Om het contract duidelijk te maken, worden de afspraken die zijn vastgelegd tussen de partijen op een zodanige manier geformuleerd dat in de toekomst alle afspraken nog steeds op de juiste wijze worden geïnterpreteerd. Voornoemde is van belang om geschillen en misverstanden te voorkomen. Het contract moet ook legaal zijn. Het contract met de algemene voorwaarden mag niet in strijd zijn met de wetgeving, openbare orde en goede zeden.[106]

5.3.4 Fase 4: Creatieregister

Het creatieregister kan worden gebruikt om volledigheid te bevorderen en om duidelijkheid te creëren over de te volgen en de werkelijk gevolgde procedure van het contracteren. In het creatieregister moet de verantwoordelijke worden opgenomen.[107]

5.3.5 Fase 5: Beoordeling

Om goede contracten te bewerkstelligen is een beoordeling door anderen dan de contractopstellers gewenst. De contracten moeten de juridische toets doorstaan en financieel verantwoord zijn. Daarnaast is het wenselijk en in sommige gevallen noodzaak dat het af te sluiten contract in lijn met de strategie van de organisatie ligt.[108]

5.3.6 Fase 6: Autorisatie

Als de beoordeling vanuit de organisatie akkoord is en als beide partijen akkoord zijn gegaan met de inhoud van het contract, kan er getekend worden. Contracten zijn niet altijd van hetzelfde soort. Binnen het autorisatiebeleid moet daarom duidelijk naar voren komen wie bevoegd is om het contract te autoriseren. Voornoemde kan eenvoudig worden gerealiseerd door het categoriseren van de contracten en de verschillende contractcategorieën te koppelen aan een functionaris die bevoegd is om te tekenen voor de desbetreffende contractcategorie. Daarnaast moet dit beleid eenduidig gecommuniceerd worden naar de medewerkers van de organisatie. Zo kan er uiteindelijk worden gestreefd naar een standaardisatie van het systeem, waarbij standaardcontracten en algemene voorwaarden eenmaal juridisch getoetst worden. Bij andere (individuele) contracten behoeven dan alleen nog maar de bepalingen juridisch te worden getoetst die afwijkend zijn van de standaardcontracten. Individuele contracten die voor het eerst worden afgesloten en in de toekomst wellicht vaker worden afgesloten worden zo eenmalig ingevoerd in het systeem onder de toebehorende categorie. Door deze procedure van autorisatie te volgen wordt het duidelijk welke weg het contract moet volgen binnen de organisatie en wordt duidelijk welke functionaris bevoegd is tot autorisatie. Het beoordelingsbeleid en het autorisatiebeleid kunnen uiteindelijk gezamenlijk tot één geheel worden gevormd.[109]

5.3.7 Fase 7: Contractenregister

Door het registeren van de geautoriseerde contracten wordt er een contractenregister gerealiseerd. Het contractenregister vormt een informatieverzameling van alle contracten en andere belangrijke gegevens die van toepassing zijn op de contracten, zoals het soort contract, leverancier, interne afnemer, data, status en soort product/ dienstverle-

[105] T. Knoester, *Management in de praktijk,* Houten: Bohn Stafleu van Loghum, 2005, p. 39-43.
[106] V.S.M. Hijl, D. Van der Meer, *Contractbeheer, Theorie in praktijk*, Heerde: Mercante Publishing, 2002, p. 42-44.
[107] V.S.M. Hijl, D. Van der Meer, *Contractbeheer, Theorie in praktijk,* Heerde: Mercante Publishing, 2002, p. 44.
[108] V.S.M. Hijl, D. Van der Meer, *Contractbeheer, Theorie in praktijk*, Heerde: Mercante Publishing, 2002, p. 44.
[109] V.S.M. Hijl, D. Van der Meer, *Contractbeheer, Theorie in praktijk,* Heerde: Mercante Publishing, 2002, p. 44-45.

ning.[110] Wat er allemaal in contractenregister wordt opgenomen is aan de organisatie zelf, gezien elke organisatie een andere informatiebehoefte heeft. Contracten die worden geregistreerd in het register moeten allemaal een uniek nummer krijgen, zodat de desbetreffende contracten altijd herleidbaar en te identificeren zijn. Naast de contracten kunnen de markt- en ervaringsinformatie ook worden opgeslagen in het register. Bijvoorbeeld kan gedacht worden aan de gegevens van de wederpartij. Door het opzetten van een contractenregister en de contracten daar te registeren kunnen de verschillende contractactiviteiten, vervaldata en de contractbewaartermijn goed in de gaten worden gehouden.

Het creatieregister en het contractenregister kunnen worden samengevoegd door de organisatie. Het samengevoegde register bevat dan alle gegevens van contracten vanaf het eerste moment van registratie tot het moment dat het contract ten einde loopt en kan worden gearchiveerd. Het eventuele nadeel wat ontstaat door het samenvoegen is, dat beide registers niet individueel meer kunnen worden gecontroleerd op volledigheid. Wordt de keuze gemaakt om de registers gescheiden te houden. Dan blijven beide registers aan elkaar verbonden. Immers elk contract dat in het creatieregister wordt opgenomen en uiteindelijk moet worden geautoriseerd, moet worden opgenomen in het contractenregister. Andersom geldt dat als een contract in het contractenregister wordt opgenomen, met de gevolgde werkprocedure, het contract tevens in het creatieregister moet worden opgenomen.[111]

5.3.8 Fase 8: Archiveren

De contracten (originele exemplaren) moeten worden gearchiveerd in het daartoe bestemde archief van de organisatie. De originele exemplaren dienen namelijk te worden gescheiden van het werkdossier, vanwege de veiligheid. Het archief dient er namelijk voor, dat de contracten worden beschermd tegen fysieke calamiteiten zoals brand, waterschade etc.[112] Het archief van de contracten mag alleen toegankelijk zijn voor de daartoe bevoegde personen, waar de bevoegde personen de contracten in het archief op een eenvoudige manier kunnen lokaliseren en archiveren. De eenvoudige lokalisatie kan worden gecreëerd door het invoeren van eenzelfde systeem als de nummering in het contractenregister. Het streven naar één centraal archief is niet noodzakelijk. Wordt er echter gebruikgemaakt van meerdere archieven, dan is het wel zeer wenselijk om de locatie van het desbetreffende te archiveren contract te vermelden in het daartoe bestemde registratieregister. Door het voeren van meerdere archieven wordt de beheersbaarheid van het archief wel complex gemaakt. Kortom, een goede registratie is een pre.[113]

5.3.9 Fase 9: Generatie en distributie van gegevens

Bij de uitvoering van werkzaamheden is het soms nodig om gegevens uit contracten te kunnen raadplegen. De informatie die men nodig heeft, zijn vaak kopieën van contracten, gegevens van contracten en over de contracten zelf. Vaak is die informatie niet kant-en-klaar en moet daarom worden gegenereerd en gedistribueerd. Gedacht kan worden aan een selectielijst van leveranciers of een berekening van de betalingsverplichtingen uit contracten. In het contractregister kan worden geregistreerd wie er informatie heeft opgevraagd en waar dat naar toe is gegaan.[114]

5.3.10 Fase 10: Bewaking en beëindiging

De afspraken die tussen partijen zijn gemaakt in de contracten, moeten door de contractpartijen worden nagekomen. Worden die afspraken namelijk niet nagekomen dan is er sprake van een tekortkoming in de nakoming van de verbintenis. De tekortkoming verplicht de schuldenaar de schade die de schuldeiser daardoor lijdt te vergoeden, tenzij de tekortkoming de schuldenaar niet kan worden toegerekend, oftewel wanprestatie op grond van artikel 6:74 BW. Het is dus erg zinvol om de nakoming actief te bewaken. De

[110] Publicatie NPPP, *Contractbeheer en contractmanagement*, juni 2004

[111] V.S.M. Hijl, D. Van der Meer, *Contractbeheer, Theorie in praktijk*, Heerde: Mercante Publishing, 2002, p. 45.

[112] J. Van Tiggelen, 'Archiveren', *Handboek Administratie,* oktober 1993. pp. A5570.

[113] V.S.M. Hijl, D. Van der Meer, Contractbeheer, *Theorie in praktijk, Heerde*: Mercante Publishing, 2002, p. 45-46.

[114] V.S.M. Hijl, D. Van der Meer, Contractbeheer, *Theorie in praktijk, Heerde:* Mercante Publishing, 2002, p. 46.

verantwoordelijke functionaris moet controleren of de wederpartij zich aan de opgestelde verplichtingen houdt en daarnaast moet de functionaris de termijnen voor het uitvoeren van activiteiten die aflopen bewaken.

Om goede uitvoeringen en beëindiging van contracten te waarborgen, is er informatie nodig over de vereiste activiteiten en bijhorende datum. De desbetreffende informatie kan normaliter in het contractenregister worden gevonden, mits deze goed wordt bijgehouden. Effectieve bewaking kan ook pas worden gegarandeerd als degene die de activiteiten heeft uitgevoerd of de contracten heeft beëindigd dit meldt of registreert in het contractenregister. Door het voeren van informatie die correcte en up-to-date is, kan de bewaking van de contracten eenvoudig worden gerealiseerd en uitgevoerd worden.[115]

5.3.11 Fase 11: Uitvoering

De contractpartijen moeten er zorg voor dragen dat de juiste prestatie met de juiste kwaliteit, op het juiste moment, op de juiste plaats en in de juiste hoeveelheid worden uitgevoerd. Dit kan gecheckt worden op basis van de informatie die is overeengekomen, vastgelegd en ondertekend is. Om de doelstellingen te realiseren van de uitvoeringsfase is informatie nodig uit het contract. Dit betekent dat de benodigde informatie te allen tijde beschikbaar moet zijn en daarnaast moet het contract duidelijk en volledig worden opgesteld om onduidelijkheden te voorkomen. Dit doet de uitvoerbaarheid van de contracten ten goede.[116]

5.3.12 Fase 12: Beëindiging en nazorg

Vaak verloopt de beëindiging van een contract min of meer vanzelf. In veel gevallen is het namelijk zo, dat de prestaties zijn verricht of dat de contractdatum ten einde loopt. Het is echter niet in alle gevallen zo vanzelfsprekend dat de contracten ten einde lopen. In deze gevallen moet de beëindiging worden gedaan door middel van een expliciete handeling, die op het juiste moment uitgevoerd moet worden.[117] De bewakingstermijn omtrent beëindiging moet daarom adequaat in de gaten worden gehouden. Voor het beëindigen van het contract is informatie uit het contract, informatie over de behoefte van de organisatie en over de juridische mogelijkheden nodig.

Een goede nazorg kan worden gewaarborgd door het houden van een evaluatie van de beëindiging en registratie van de ervaringen die zijn opgedaan tijdens de contractperiode. Dit leidt namelijk tot een goed oordeel over de contracten, alsook over de wederpartij. Als bijvoorbeeld achteraf blijkt dat de contracten toch niet aan de kwaliteitseisen voldoen of de wederpartij heeft verzuimd, kunnen daar maatregelen voor worden genomen om dit in de toekomst te voorkomen. Een goede nazorg leidt daarom tot waardevolle ervaringsinformatie.[118]

5.3.13 Fase 13: Volledigheidcontrole

De volledigheidscontroles kunnen worden gehouden door de inhoud van de creatieregisters met die van het contractenregister te vergelijken. Daarnaast kan er ook informatie worden verzameld uit de organisatie zelf en die vergelijken met het contractenregister.[119]

5.3.14 Fase 14: Inrichting en opschoning archief en registers

Om een goede structuur in het archief en de registers te behouden is een periodieke opschoning noodzakelijk. Het is daarom van belang de kenmerken van informatieverzamelingen en de informatiebehoefte in de organisatie te kennen en de vervallen documenten te verwijderen uit het archief en de registers. Dit, om te voorkomen dat het archief en de registers overvol en onbeheersbaar raken. Dergelijke informatie omtrent opschoning en herinrichting kan in de contractenregister worden opgenomen.[120]

[115] V.S.M. Hijl, D. Van der Meer, Contractbeheer, *Theorie in prak tijk, Heerde*: Mercante Publishing, 2002, p. 46.
[116] V.S.M. Hijl, D. Van der Meer, *Contractbeheer, Theorie in praktijk*, Heerde: Mercante Publishing, 2002, p. 47.
[117] Publicatie NPPP, *Contractbeheer en contractmanagement*, juni 2004.
[118] V.S.M. Hijl, D. Van der Meer, *Contractbeheer, Theorie in praktijk*, Heerde: Mercante Publishing, 2002, p. 47.
[119] V.S.M. Hijl, D. Van der Meer, *Contractbeheer, Theorie in praktijk*, Heerde: Mercante Publishing, 2002, p. 47.
[120] V.S.M. Hijl, D. Van der Meer, *Contractbeheer, Theorie in praktijk*, Heerde: Mercante Publishing, 2002, p. 47.

5.4 Organisatie van het contractbeheerproces

Het contractbeheerproces is een beschrijving van de mogelijke vormgeving van het contractbeheer, waar de belangrijkste basisactiviteiten en informatieverzamelingen in op zijn genomen. De organisatie kan zelf invullen in hoeverre en op welke wijze de verschillende fasen worden uitgevoerd. Het beschreven contractbeheerproces kan worden geïnterpreteerd als een kader waarbinnen het contractbeheer van het UMCG kan worden gerealiseerd.

Per activiteit zal het UMCG ook moeten bepalen wie voor de uitvoering verantwoordelijk wordt gesteld. De vraag die daarom gesteld kan worden luidt: in welke mate worden de verschillende activiteiten uitgevoerd: decentraal of centraal? De activiteiten kunnen het beste worden uitgevoerd op het organisatieniveau waar de beste inhoudelijk kennis is en waar overzicht is over de genomen beslissingen. Anderzijds, als er centraal contractbeheer is wordt het overzicht over de wijze waarop de activiteiten plaatsvinden en de resultaten die daaruit voortvloeien vergroot.

Het activiteitenproces van het contractbeheer kan worden onderverdeeld in een drietal groepen:

1. Contract specifieke eisen: wat betekent dat de activiteiten specifiek per contract zijn en specifieke kennis is vereist voor die contracten zoals selecteren van de wederpartij, uitvoeren en beëindigen etc.;
2. Contractgroep gebonden eisen: wat betekent dat de activiteiten voor een groep contracten op een eenduidige manier kunnen plaatsvinden zoals generen en distribueren van informatie, inrichten decentrale registers etc.;
3. Contract overstijgende eisen: wat betekent dat de activiteiten uitgevoerd kunnen worden voor alle contracten in de organisatie zoals het beoordelen, autoriseren, registreren, archiveren etc.

Om goed contractbeheer te realiseren moet er dus een verantwoordelijke voor de uitvoering van de verschillende activiteiten in het leven worden geroepen. Uit de literatuur blijkt dat daar twee functies voor zijn, namelijk de contractenbeheerder en de contractencoördinator. Beide functies worden in de volgende paragrafen besproken.[121]

5.4.1 De contractenbeheerder

De contractenbeheerder is verantwoordelijk voor één groep of meerdere groepen contracten. Desondanks heeft elke groep maar één verantwoordelijke beheerder. De functie van de contractenbeheerder houdt ten eerste in, dat hij moet zorgen dat er wordt voldaan aan de standaardisatie-eisen die voor het contractgroep overstijgende niveau worden gesteld en ten tweede dat hij ervoor moet zorgen dat alle contractgroep gebonden activiteiten op een goede wijze worden uitgevoerd. De contractenbeheerder moet voor decentralisatie kiezen met betrekking tot de procesgebonden activiteiten. Dit, omdat hij anders een te grote taak heeft. Wat betekent dat de werkzaamheden van de contractenbeheerder te omvangrijk worden (zie voor de specifieke functies van de contractenbeheerder bijlage 5).[122]

5.4.2 De contractencoördinator

De contractencoördinator is verantwoordelijk voor alle groepsoverstijgende activiteiten. De contractencoördinator kan centraal op een gestandaardiseerde manier de activiteiten laten uitvoeren of hij kan die activiteiten decentraal laten uitvoeren. In alle gevallen geeft hij aan binnen welke kaders moeten worden gehandeld ten aanzien van de standaardisatie en dat de procedures goed door de verantwoordelijken worden uitgevoerd (zie voor de specifieke functies van de contractencoördinator bijlage 5).[123]

5.5 Conclusie

Contractbeheer zorgt ervoor dat de juiste informatie op het juiste tijdstip op de juiste plaats is, ter ondersteuning van het gehele contracteringsproces. Dit betekent kortgezegd dat de informatie kan bestaan uit het contract zelf,

---

[121] V.S.M. Hijl, D. Van der Meer, *Contractbeheer, Theorie in praktijk,* Heerde: Mercante Publishing, 2002, p. 55-60.
[122] V.S.M. Hijl, D. Van der Meer, *Contractbeheer, Theorie in praktijk,* Heerde: Mercante Publishing, 2002, p. 60-61.
[123] V.S.M. Hijl, D. Van der Meer, Contractbeheer, Theorie in praktijk, Heerde: Mercante Publishing, 2002, p. 61-62.

maar ook uit informatie van het contract of informatie over het contract. Het contractbeheer an sich bestaat uit 14 fasen. De fasen kunnen op hoofdlijnen worden onderverdeeld in:

- sluiten van contracten (specifiëren, selecteren en contracteren);
- registratie van de contracten (contractbeheer);
- managen van de uitputting en mutatie bij wijzigingen van contracten (management van contracten);
- bewaken van de contracten (verlengen en beëindigen).

Tot slot is het van belang dat het contractbeheer wordt nageleefd door alle medewerkers van het UMCG en daarnaast dat er EPV bewustwording word gecreëerd. Het volgende hoofdstuk gaat hier verder op in.

5.6 Onderzoekspunten

De onderzoekspunten uit dit hoofdstuk zijn:

- *Wat is de huidige infrastructuur van het contractbeheer binnen de sectoren/ afdelingen van het UMCG?*
- *Kan het contractbeheer binnen de sectoren/ afdelingen idealiter functioneren?*
- *Worden er contracten gesloten met derden? En zo ja, welke?*
- *Zijn de verantwoordelijke functionarissen m.b.t. contracten duidelijk?*
- *Is de autorisatie m.b.t. contracten duidelijk en hoe functioneert dat binnen het UMCG?*

6 COMPLIANCE EN IMPLEMENTATIE WET- EN REGELGEVING

6.1 INLEIDING

Dit hoofdstuk vormt het slotstuk van de theorie. Het antwoord op de laatste theoretische deelvraag kan daarom worden geformuleerd. Compliant en implementatie wet- en regelgeving is een belangrijk onderdeel van dit onderzoek. De EPV is immers een nieuwe verordening waar het UMCG op het moment mogelijk niet aan voldoet.
De laatste theoretische deelvraag luidt:

- *Wat is volgens de (juridische) literatuur een goede methode om nieuwe wet- en regelgeving binnen een organisatie te implementeren?*

Achtereenvolgens worden de volgende onderwerpen besproken: compliance (§ 6.2), de compliancecyclus (§ 6.3) en tot slot de conclusie (§ 6.4) en onderzoekspunten (§ 6.5).

6.2 COMPLIANCE

Compliance betekent dat een persoon of organisatie werkt in overeenstemming met de wet- en regelgeving, kortgezegd naleving. Naast de naleving van de wet- en regelgeving duidt de term compliance ook het proces dat ertoe moet leiden dat wet- en regelgeving door de organisatie wordt nageleefd. De organisatie is dus compliant als het voldoet aan de wet- en regelgeving die van toepassing is op de activiteiten van de organisatie. Compliance heeft tegenwoordig niet alleen maar betrekking op de wettelijke regels die door de overheid worden opgelegd. Het begrip compliant betreft een bredere interpretatie en betreft qua regelgeving ook naleving van maatschappelijke en ethische normen, vertaald naar de eigen regels van de organisatie. Met andere woorden betekent compliance het (goed) functioneren van de organisatie.[124]

Als een organisatie niet compliant is aan de wet- en regelgeving brengt dat de nodige risico's met zich mee. Een risico in het kader van de EPV zijn de sancties bij niet-naleving. Een goed ondernemingsbestuur is daarom nodig, gezien zo de risico's verbonden aan de ondernemingsactiviteiten worden beheerst. Naast de boete, die bijvoorbeeld toezichthouder het CBP kan geven, kunnen er ook andere gevolgen denkbaar zijn zoals reputatieschade, milieurisico's, bedrijfsveiligheid, terrorismerisico en aansprakelijkheidsrisico's. Compliance kan daarom worden neergezet als een instrument om risico's goed te kunnen beheersen. Een adequate beheersing van de compliantrisico's vergt wel een investering van de organisatie. Veel organisaties zien compliance vaak als overhead en wat daarom veel geld gaat kosten. Veelal is het zo dat de kosten ten gevolge van een compliance-incident vele malen hoger zijn, in vergelijking met de nodige investering om compliance te implementeren in de bedrijfsvoering en daardoor de risico's beheersbaar maken.[125]

Compliance staat daarom in een directe lijn met risicomanagement, waardoor de twee definities met elkaar zijn verbonden. Risicomanagement vertaalt zich naar het bundelen en coördineren van het management van bedrijfsorganisatie door de hele organisatie. Compliance richt zich op naleving van regels met als doel om de risico's beheersbaar te maken en schade die voortvloeit uit de risico's zoveel mogelijk te beperken. Het 'in control' brengen van een organisatie is het doel van ziekenhuis compliance en risicomanagement. Compliance en risicomanagement levert het ziekenhuis verscheidene voordelen op. Zo ontstaat er meer inzicht in relevante externe wet- en regelgeving, alsook richtlijnen, procedures, instructies en interne regelementen van het ziekenhuis. De toegankelijkheid van de richtlijnen, procedures, instructies en interne regelementen wordt verbeterd voor het ziekenhuis, alsook het toezicht.

[124] B.H.A. van Leeuwen, A.G.H. van der Staay & O. Javornik,, *beroep: Bedrijfsjurist, Praktische leidraad voor bedrijfsjuristen*, Deventer: Kluwer, 2009, p. 95-96.

[125] B.H.A. van Leeuwen, A.G.H. van der Staay & O. Javornik,, *beroep: Bedrijfsjurist, Praktische leidraad voor bedrijfsjuristen*, Deventer: Kluwer, 2009, p. 97-102.

Daarnaast is er minder overlap in interne regelementen, richtlijnen en procedures. De EPV vraagt de verantwoordelijke van het UMCG overzicht van alle verwerkingen van persoonsgegevens te kunnen aantonen en wat is afgesproken omtrent de verantwoordelijkheid ten aanzien van die verwerkingen. Het laatste voordeel wat daardoor gecreëerd kan worden, is dat compliance en risicomanagement het ziekenhuis de mogelijkheid biedt om transparant te rapporteren aan de belanghebbende over de naleving van de externe wet- en regelgeving en interne reglementen, richtlijnen, procedures en instructies.[126] Kortom kan er worden gekomen tot de volgende beschrijving omtrent ziekenhuis compliance en risicomanagement:
"Ziekenhuis compliance 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. "[127]

6.3 De compliancecyclus

6.3.1 De methode voor implementatie van regelgeving

Om als organisatie compliant te worden aan nieuwe wetgeving, is een methode nodig om dat te bewerkstelligen. De EPV stelt dat in de gegevenshuishouding ten behoeve van de bedrijfsvoering 'privacy by design' en privacy by default'[128] moeten worden ingebouwd. De methode die hiervoor gebruikt kan worden is de compliancecyclus. De compliancecyclus is een methode om een bepaalde regeling binnen een organisatie te implementeren aan de hand van een afzonderlijk project. In het kader van de EPV kan een PDCA-cyclus in de verwerking/ gegevenssysteem worden geïmplementeerd die moeten worden gemonitord en beheerd. De compliancecyclus heeft naast de functie van implementatiemethode, ook de functie om de effectiviteit te bewaken en waar nodig te verbeteren. In deze paragraaf wordt de methode, met de vier fasen, nader uitgewerkt om een goede implementatie van nieuwe wetgeving in de organisatie te bewerkstelligen. Het proces van de compliancecyclus bestaat uit de volgende vier fasen:

1. plannen;
2. regels maken en implementeren;
3. toezien op naleving;
4. verbeteren.

In de vier fasen van de compliancecyclus, zijn de vier stappen van de PDCA-cirkel[129] te herkennen: Plan, Do, Check, Act. De PDCA-cirkel is door de kwaliteitsdeskundige E. Edward Deming ontwikkeld als verbetercirkel voor kwaliteitsmanagement. Vele methoden zijn afgeleid van de Deming-cirkel, waar ook de compliancecyclus. Kortom, de compliancecyclus is een kwaliteitstraject voor de naleving van wet- en regelgeving.

De compliancecyclus is een iteratief proces, wat betekent dat de cyclus als maar weer opnieuw kan worden ingevuld en continue op verbetering is gericht. Als blijkt dat na de vierde fase van de cyclus de organisatie heeft gefaald op de invoering van de effectiviteit of dat de organisatie de regels niet heeft nageleefd, kunnen er nieuwe maatregelen worden ingevoerd. Bij het invoeren van nieuwe maatregelen gaat een nieuwe cyclus van start, die mogelijk weer leidt tot verbetering van de effectiviteit en de naleving van de regels binnen de organisatie. Voor het complianceproject is het naast een goede invulling van de compliancecyclus, het ook cruciaal dat het bestuur van de organisatie de compliance serieus in acht neemt en op een positieve manier actief uitdraagt naar de organisatie. [130]

Het compliancetraject succes hangt dus niet alleen af van een goed doordacht project, waarin de methode tot in de puntjes is uitgewerkt om naleving van nieuwe wet- en regelgeving te realiseren. De omgevingsfactoren hebben een prominente rol om het compliancetraject te laten slagen.

---

[126] S.C. Bleker-van Eyk, 'Het belang van compliance voor ziekenhuizen', *VU Magazine, Compliance & Integriteit*, nr. 3, december 2010, p.8.

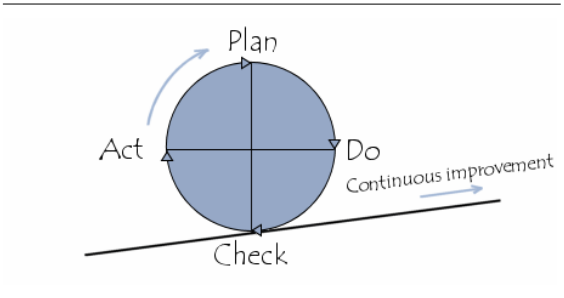
[127] S.C. Bleker-van Eyk, 'Het belang van compliance voor ziekenhuizen', *VU Magazine, Compliance & Integriteit*, nr. 3, december 2010, p.6.

[128] Zie § 4.8 voor uitleg van het begrip 'privacy by design' en privacy by default'.

[129] Figuur 2.

[130] B.H.A. van Leeuwen, A.G.H. van der Staay & O. Javornik,, *beroep: Bedrijfsjurist, Praktische leidraad voor bedrijfsjuristen*, Deventer: Kluwer, 2009, p. 104-106.

Het resultaat van alle betrokkenen binnen de organisatie is namelijk leidend voor een goed slagen van het compliancetraject: de organisatiecultuur.[131] De cultuur van de organisatie is veelal een 'tone-at-the-top'. Het bestuur en het management van de verschillende bedrijfsonderdelen hebben een voorbeeldfunctie: goed voorbeeld doet volgen. Omgekeerd is het echter ook veelal aan de orde: slecht voorbeeld doet volgen. Het commitment en de onvoorwaardelijke support van het bestuur is daarom voor het compliancetraject noodzakelijk. Compliance is immers een belangrijk onderdeel van de organisatie om beoogde doelen te halen en daarnaast tot een goed slagen te leiden.[132]



Figuur 2 Compliancecyclus

6.3.2 Fase 1: Plannen

In de eerste fase worden de voorbereidingen voor alle fasen in de cyclus getroffen, waardoor de planningsfase een belangrijk onderdeel is van de cyclus. Het resultaat van de planningsfase is een doordacht plan van aanpak voor een goede uitvoering van fase 2, 3 en 4 waarin de activiteiten van de fasen zo gedetailleerd mogelijk zijn omschreven. Dit plan van aanpak kan worden genoemd als het complianceprogramma. Het complianceprogramma bestaat uit de activiteiten die door de organisatie dienen te worden uitgevoerd, om te leiden tot het realiseren van de complianceambitie omtrent de desbetreffende regeling. Kortom, het complianceprogramma zorgt er voor dat er voorbereidingen worden getroffen voor de verschillende fasen van de cyclus en dat duidelijk is wie wat doet, op welke wijze en wanneer. Het uiteindelijke doel van het complianceprogramma is het naleven van de regeling door de betrokkenen binnen de organisatie. De planningen van fase 2, 3 en 4 worden in de desbetreffende subparagrafen besproken.[133]

Stappen fase 1:

- *Inventarisatie van de voorschriften uit de regeling.*
  Allereerst moeten de vereisten waar de organisatie op grond van de regeling aan moet voldoen in kaart worden gebracht. De wettelijke normen van de regeling zijn niet altijd duidelijk voor de organisatie. De normen kunnen dan worden geïnterpreteerd op basis van de Memorie van Toelichting, wetgeschiedenis, beleidsregels van toezichthouders en jurisprudentie. Dit kan vervolgens worden uitgewerkt in door de organisatie of een bepaalde afdeling op maat gemaakte voorschriften. Als eenmaal helder is welke eisen de regeling stelt, dan kan worden bepaald welke maatregelen er kunnen worden genomen in het complianceprogramma.

- *Inventarisatie van ondernemingsactiviteiten die door de regeling worden geraakt.*
  Voorts moet worden vastgesteld welke ondernemingsactiviteiten, bedrijfs- of productieprocessen worden geraakt door de regeling. In een normenkader kunnen de verzamelende gegevens schriftelijke worden vastgelegd, waardoor een compleet beeld ontstaat van de uit de regeling voortvloeiende voorschriften en de bedrijfsdelen die worden geraakt. Voor een goed beeld is er een voorbeeld normenkader opgenomen in bijlage 6.

- *Identificeren en analyseren van de risico's van niet-naleving.*
  Vervolgens kan de eerste inhoudelijke stap van het complianceproces worden gezet: het in kaart brengen en analyseren van de risico's die niet-naleving van de

[131] B.H.A. van Leeuwen, A.G.H. van der Staay & O. Javornik,, *beroep: Bedrijfsjurist, Praktische leidraad voor bedrijfsjuristen*, Deventer: Kluwer, 2009, p. 106.

[132] B.H.A. van Leeuwen, A.G.H. van der Staay & O. Javornik,, *beroep: Bedrijfsjurist, Praktische leidraad voor bedrijfsjuristen*, Deventer: Kluwer, 2009, p. 122.

[133] B B.H.A. van Leeuwen, A.G.H. van der Staay & O. Javornik,, *beroep: Bedrijfsjurist, Praktische leidraad voor bedrijfsjuristen*, Deventer: Kluwer, 2009, p. 107.

regeling met zich meebrengen in de organisatie. De analyse is gericht op de vragen als: waar en wanneer doet deze zich voor, hoe groot is de kans op een risico en wat is de impact als het risico tot uiting komt binnen de organisatie? Als de risico's zijn geanalyseerd worden ze schriftelijk vastgelegd, bestaande uit een beschrijvend deel verwerkt in een risicomatrix. Door de risicomatrix worden compliancerisico's inzichtelijk gemaakt en kan bij niet-naleving het risico eenvoudig worden beoordeeld. Voor een goed beeld is er een voorbeeld risicomatrix met uitleg opgenomen in bijlage 7.

- *Vaststellen van de complianceambitie.*
  De organisatie kan nu bepalen welke resultaten gehaald moeten worden op grond van de vastgelegde compliantrisico's van de regeling. Daarbij dienen de doelstellingen te worden geformuleerd en de maatstaven te worden gedefinieerd. Uit voornoemde kan dan worden opgemaakt of de organisatie de doelstellingen heeft gehaald.

- *Bepalen van maatregelen ter beheersing van het risico van niet-naleving.*
  Er zijn maatregelen nodig om de compliancerisico's te kunnen beheersen. Deze maatregelen zijn gericht om de naleving van de regeling te realiseren en betreffen het beleid dat wordt uitgewerkt in fase 2. In fase 2 worden namelijk de instructies en procedures, de wijze waarop de regels worden ingevoerd, de nalevingscontroles en de acties tot het verbeteren van de maatregelen verwerkt. Het systeem van maatregelen moet op de organisatie worden afgestemd. Afhankelijk van de complexiteit en de grootte van de organisatie zal het systeem van maatregelen meer op hoofdlijnen of meer gedetailleerd kunnen worden uitgewerkt. Het is wel van belang dat het systeem zo wordt ingericht dat de verantwoordelijken duidelijk zijn vastgelegd.[134]

- *Vaststellen van een tijdpad met deadlines.*

- *Bepalen welke personen verantwoordelijk zijn voor uitvoering.*

- *Bepalen of er externe deskundigheid of ondersteuning moet worden ingehuurd.*

- *Opstellen van een budget voor het compliancetraject.*

- *Opstellen (ontwerp) complianceprogramma.*

6.3.3 Fase 2: Regels maken en implementeren

Voor fase 2 van de cyclus moeten de volgende stappen in de planningsfase worden opgenomen en uitgewerkt.

Stappen planning fase 2:

- *Het vertalen van de regels naar begrijpelijke instructies en procedures.*
  In de tweede fase is de eerste stap het maken van regels. Daarmee wordt bedoeld om de voorschriften van de regeling te vertalen naar de interne beleidsregels, begrijpelijke instructies en/of procedures. De bedoeling van die vertaling is om het risico van niet-naleving in controle te houden. Daarnaast is het van belang dat duidelijk wordt welke personen gemoeid zijn met de naleving van de desbetreffende regeling en wat daarvoor moet gebeuren. Het uitgangspunt is dat de regels zo geformuleerd moeten worden, dat het voor de betrokkenen in de organisatie op een eenduidige en heldere manier kan worden geïnterpreteerd.

- *Het implementeren van de regels in de organisatie.*
  Naast het opstellen van de regels, moeten de regels natuurlijk worden nageleefd binnen de organisatie. Door het opstellen van een goed doordacht plan om de regels en procedures binnen de organisatie te implementeren is naleving te bewerkstelligen. Het uitgangspunt van het plan is, dat duidelijk wordt hoe bereikt kan worden dat de betrokkenen die gemoeid zijn met de regels op de hoogte zijn en wat die betrokkenen moeten doen om ervoor te zorgen dat de regels op een juiste wijze worden nageleefd. Dit kan gerealiseerd worden door goede communicatie, training en het creëren van bewustwording.

[134] B.H.A. van Leeuwen, A.G.H. van der Staay & O. Javornik,, *beroep: Bedrijfsjurist, Praktische leidraad voor bedrijfsjuristen*, Deventer: Kluwer, 2009, p. 108-112.

- *Communicatie en training.*
  Een tijdige en heldere communicatie is tijdens de communicatie- en trainingsplanning een belangrijk punt van aandacht. De planners van de organisatie kunnen daar alvast een communicatieplan voor opstellen. Bij de planning van de communicatie en training moet besloten worden wanneer en op welke manier de communicatie tot stand moet komen, ten aanzien van de in de organisatie te voeren nieuwe compliance-eisen.

- *Creëren van bewustwording.*
  Bewustwording is naast de communicatie een belangrijk aspect om naleving van de nieuwe regeling te realiseren. Tijdens de planning moet het creëren van bewustwording daarom aandacht verdienen en concreet worden ingevuld. Dit gezien bewustwording vaak als een lastige taak wordt ervaren binnen een organisatie. Bij het creëren van bewustwording is de voornaamste en belangrijkste taak te bepalen wie uiteindelijk verantwoordelijk is voor de naleving van de compliance-eisen. Tot slot moet er ook aandacht worden besteed aan hoe kan worden bereikt dat de doelgroepen zich bewust worden, dat naleving van de regels noodzakelijk is en daarnaast van groot belang is voor de organisatie.[135]

Uitvoering.
Op basis van het complianceprogramma worden de activiteiten binnen fase 2 met betrekking tot het maken en implementeren van de regels uitgevoerd binnen de daarvoor gestelde termijn.[136]

6.3.4 Fase 3: Toezien op naleving

Voor fase 3 van de cyclus moeten de volgende stappen in de planningsfase worden opgenomen en uitgewerkt. In de planning van fase 3 moet aandacht worden besteed aan het toezicht op naleving van de regeling. Dit betekent dat gekeken moet worden hoe de instructies en procedures het beste kunnen worden gecontroleerd, hoe vaak dit kan worden gecontroleerd, hoe moet worden gecontroleerd en op welke wijze de bevindingen van de controle worden teruggekoppeld of gerapporteerd. De wijze van controle is vrij, echter moet het toezicht wel gericht zijn op het achterhalen van niet-naleving of tekortkomingen in het complianceprogramma. Dit alles is van belang, omdat zo het bestuur tijdig kan worden ingelicht en daarnaast dat het bestuur adequaat kan bijsturen. Immers niet-naleving kan alleen worden geconstateerd door middel van een gedegen controle. Mist een controle, dan functioneert het complianceprogramma logischerwijze niet optimaal.

Stappen planning fase 3:
- *Bepalen van vorm, frequentie en intensiteit van het toezicht op naleving.*
  De vorm, frequentie en intensiteit van de controles kan worden getoetst aan de hand van de omvang van de organisatie, de aard van de regels en met name de analyse van de risico's, voortvloeiend uit de risicomatrix, bij niet-naleving.

- *Prioriteiten bepalen in de monitoringsactiviteiten op basis van de risico's.*
  Bij het bepalen van de prioriteit kan een inschatting worden gemaakt van de te verwachten hoeveelheid en de te verwachting vormen van non-compliant gedrag.

- *Bepalen op welke wijze, wanneer, door wie en aan wie moe worden gerapporteerd.*

- *Bepalen hoe te handelen bij geconstateerde niet-naleving.*[137]

Uitvoering.

[135] B.H.A. van Leeuwen, A.G.H. van der Staay & O. Javornik,, *beroep: Bedrijfsjurist, Praktische leidraad voor bedrijfsjuristen*, Deventer: Kluwer, 2009, p. 112-114.
[136] B.H.A. van Leeuwen, A.G.H. van der Staay & O. Javornik,, *beroep: Bedrijfsjurist, Praktische leidraad voor bedrijfsjuristen*, Deventer: Kluwer, 2009, p. 119-120.
[137] B.H.A. van Leeuwen, A.G.H. van der Staay & O. Javornik,, *beroep: Bedrijfsjurist, Praktische leidraad voor bedrijfsjuristen*, Deventer: Kluwer, 2009, p. 115-117.

In fase 3 van de compliancecyclus zijn de regels binnen de organisatie geïmplementeerd en werkt de organisatie volgens de regels. Instrumenten om de implementatie te monitoren zijn onder andere softwaresystemen en ICT. Tegenwoordig zijn er steeds meer technologische methodes voor monitoring en meting van compliance. Gedacht kan worden aan GRC-software: Goverance, Risk and Compliance. Daarnaast is het raadzaam om de complianceinspanningen en de mate van wet- en regelgeving naleving vast te leggen. Dit om het toetsbaar te maken voor toezichthouders of rechters.[138] '

6.3.5 Fase 4: Verbeteren

Voor fase 4 van de cyclus moeten de volgende stappen in de planningsfase worden opgenomen en uitgewerkt. In de planning van fase 4 staat het evalueren en verbeteren centraal. Hier wordt gekeken of de compliancedoelstellingen zijn gehaald.

Stappen planning fase 4:

- *Bepalen wie verantwoordelijk is voor de beoordeling van de rapportages en de evaluatie van de complianceprestaties.*
- *Vaststellen aan de hand van welke criteria bepaald wordt welke maatregelen, instructies of procedures verbetering behoeven.*
- *Vaststellen van het tijdstip waarop de evaluatie en aanbevelingen gereed moeten zijn.*
- *Bepalen wie de actiepunten naar de planners communiceert.*
- *Bepalen door wie en hoe wordt bewaakt dat aanbevelingen en actiepunten worden opgevolgd.*[139]

Uitvoering

Op basis van de gegevens of rapportages uit fase 3 kan de cyclus worden beoordeeld op in welke mate de compliancedoelstelling uit fase 1 is behaald. Als blijkt dat de doelstelling niet is gehaald, kan er worden bijgestuurd. Het bijsturen kan door het aanvullen of verbeteren van bestaande regels en in het ergste geval het opstellen van nieuwe regels. Daarnaast kan worden onderzocht waarom de doelstelling niet is behaald ten aanzien van waar het fout ging, de ernst van de fout en waarom het fout ging. Uiteindelijk kunnen er conclusies worden getrokken, waar aanbevelingen op worden geformuleerd. De aanbevelingen moeten dan worden gecommuniceerd aan het team dat belast is met de planning. Dat team moet de verbetermaatregelen formuleren, wat uiteindelijk weer leidt tot een nieuw compliancecyclus. [140]

6.4 Conclusie

Voor het implementeren van nieuwe wet- en regelgeving kan de methode van de compliancecyclus worden toegepast. De compliancecyclus is afgeleid van de PDCA-cyclus die bestaat uit vier fases: plannen, regels maken en implementeren, toezien op naleving en verbeteren. Daarnaast is de boodschap van dit hoofdstuk dat bewustwording binnen een organisatie een pre is om compliancy te realiseren.

6.5 Onderzoekspunten

De onderzoekspunten uit dit hoofdstuk zijn:

- *Is er bewustwording in het kader van de EPV?*
- *Is er bewustwording in het kader van professioneel contractbeheer?*
- *Op welke manier implementeert het UMCG nieuwe wet- en regelgeving?*

De hoofstukken 3, 4, 5 en 6 hebben een antwoord gegeven op de verschillende theoretische deelvragen. Op basis van het theoretisch kader konden de onderzoekspunten worden geformuleerd. Deze onderzoekspunten vloeien logisch voort uit de theoretische inzichten en worden meegeno-

[138] B.H.A. van Leeuwen, A.G.H. van der Staay & O. Javornik,, *beroep: Bedrijfsjurist, Praktische leidraad voor bedrijfsjuristen*, Deventer: Kluwer, 2009, p. 117-120.

[139] B.H.A. van Leeuwen, A.G.H. van der Staay & O. Javornik,, *beroep: Bedrijfsjurist, Praktische leidraad voor bedrijfsjuristen*, Deventer: Kluwer, 2009, p. 119.

[140] B.H.A. van Leeuwen, A.G.H. van der Staay & O. Javornik,, *beroep: Bedrijfsjurist, Praktische leidraad voor bedrijfsjuristen*, Deventer: Kluwer, 2009, p. 118-121.

men naar het praktijkonderzoek. Het volgende hoofdstuk gaat over de huidige bevoegdhedenregeling binnen het UMCG. Daarna volgt een hoofdstuk met de praktijkresultaten. Voor een goed overzicht treft u hieronder nog eenmaal alle onderzoekspunten aan:

- *Is het UMCG op dit moment EPV-compliant?*
- *Voldoen de standaardcontracten van het UMCG aan de EPV?*
- *Wat is de huidige infrastructuur van het contractbeheer binnen de sectoren/ afdelingen van het UMCG?*
- *Kan het contractbeheer binnen de sectoren/ afdelingen idealiter functioneren?*
- *Worden er contracten gesloten met derden? En zo ja, welke?*
- *Zijn de verantwoordelijke functionarissen m.b.t. contracten duidelijk?*
- *Is de autorisatie m.b.t. contracten duidelijk en hoe functioneert dat binnen het UMCG?*
- *Is er bewustwording in het kader van de EPV?*
- *Is er bewustwording in het kader van professioneel contractbeheer?*
- *Op welke manier implementeert het UMCG nieuwe wet- en regelgeving?*

7 HUIDIGE BEVOEGDHEDENREGELING UMCG

In dit hoofdstuk worden de algemene en specifieke bevoegdheden van de sectoren/ afdelingen uiteengezet m.b.t. overeenkomsten. Vervolgens worden de praktijkresultaten uiteengezet in hoofdstuk 8.

7.1 INLEIDING

In het kader van de sectorvorming zijn met ingang van 1 mei 2007 verantwoordelijkheden en de daarbij behorende bevoegdheden zoveel mogelijk op sectorniveau belegd. De bevoegdheden voor de sectordirecteuren gemandateerd vanuit de Raad van Bestuur, ten aanzien van contracten tekenen, worden weergegeven in dit hoofdstuk. Bij de uitoefening van de bevoegdheden worden de volgende kaders in acht genomen:

- de aanwijzingen die zijn opgenomen in de algemene bevoegdhedenregeling UMCG;
- de richtlijnen, kaders, wettelijke en interne regels die geleden voor het desbetreffende onderwerp, waaronder de CAO-UMC, en nadere instructies van de Raad van Bestuur;
- het vastgestelde budget van de sector/ het ondersteunende onderdeel;
- de instructies van die hiërarchische leidinggevende;[141]
- de uitoefening gebeurt in naam en onder verantwoordelijkheid van de Raad van Bestuur, die zelf bevoegd blijft om de bevoegdheden uit te oefenen;
- bij afwezigheid of verhindering van de bevoegde functionaris, worden diens bevoegdheden uitgeoefend door degene die is aangewezen als plaatsvervanger. Als er geen plaatsvervanger is aangewezen, dan worden de bevoegdheden uitgeoefend door de naast hogere bevoegde functionaris.

[141] Afdelingshoofden vallen hiërarchisch rechtstreeks onder de Raad van Bestuur. Dit betekent concreet dat alle rechtspositionele beslissingen ten aanzien van afdelingshoofden door de Raad van Bestuur genomen worden.

De bevoegdheden die uitgeoefend worden in naam van de Raad van Bestuur, zijn formeel te onderscheiden in de termen: mandaat (het nemen van publiekrechtelijke rechtspositionele besluiten), volmacht (het verrichten van privaatrechtelijke rechtshandelingen) en machtiging (het verrichten van handelingen die noch een publiekrechtelijke besluit noch een privaatrechtelijke rechtshandeling zijn).[142]

7.2 BEVOEGDHEDEN.

De bevoegdheden zoals het sluiten van samenwerkingsovereenkomsten en contracten (behoudens voor inhuur van externen tot een bepaald bedrag), berusten bij de Raad van Bestuur of zijn expliciet (vanwege de grote mate van specificiteit) vastgelegd in de specifieke bevoegdheidsregeling van het UMCG. In het kader van contracteren heeft de Raad van Bestuur aan de sectordirecteuren ten behoeve van hun eigen sector een aantal bevoegdheden toegekend, die nader worden uitgewerkt in de volgende paragrafen.

7.2.1 PERSONEEL EN ORGANISATIE

De sectordirecteur heeft de bevoegdheid tot het afsluiten van een (detachering)overeenkomst met een derde in het kader van uitwisselen van personeel, voor zover passend binnen het kader van de door de Raad van Bestuur afgesloten raamovereenkomsten met deze derde. Dergelijke (detachering)overeenkomsten moeten voldoen aan de eisen zoals vastgelegd in de richtlijn "BTW en juridische aspecten bij zorgprestaties, wetenschappelijk onderzoek en uitlenen/detachering".[143]

7.2.2 INKOOP

De eerste bevoegdheid van de sectordirecteur ten aanzien van inkoop is het doen van aanvragen voor bestellingen van goederen, apparatuur en diensten bij inkoop ten laste van

[142] Algemene bevoegdheidsregeling UMCG.
[143] Algemene bevoegdheidsregeling UMCG.

het budget van de sector. Bestellingen dienen altijd via inkoop te geschieden, tenzij de Raad van Bestuur schriftelijk heeft ingestemd met een afwijking van deze regel. Ten tweede heeft de sectordirecteur de bevoegdheid tot het tekenen van akkoord voor levering en akkoord voor de factuur bij bestellingen van goederen, apparatuur en diensten. Ten derde heeft de sectordirecteur de bevoegdheid om zelfstandig inkopen ten laste van het budget algemene bestedingen te doen. Tot slot heeft de sectordirecteur de bevoegdheid tot het verstrekken van een opdracht voor de inhuur van externen tot een bedrag van € 10.000,-- inclusief BTW voor zover hiervoor binnen het eigen onderdeel budget aanwezig is en voor zover de inhuur van externen niet op grond van de specifieke bevoegdhedenregeling is voorbehouden. Alle overige opdrachten vanaf € 10.000,-- inclusief BTW worden door de Raad van Bestuur verstrekt. [144]

De bevoegdheid tot het aangaan van verplichtingen met derden binnen inkoop is aan functionarissen toebedeeld. De sectordirecteur moet zich wenden tot onderstaande functionarissen. Immers inkoop heeft als corebusiness het inkopen van goederen, diensten etc. waar de inkoopfunctie wordt uitgevoerd ten behoeve en ten laste van de sector.

7.2.3 ICT

De sectordirecteur heeft de bevoegdheid tot het toekennen van bevoegdheden voor toegang/ gebruik van systemen en databases voor zover dit betrekking heeft op de eigen sector.[145]

Bevoegdheden	**Directeur Financiën & Control**	**Hoofd Inkoop**	**Senior Inkoop**	**Inkoper**
Het afsluiten van (raam)contracten.	Tot € 250.000	Tot € 100.000	Tot € 25.000	Tot € 10.000
Plaatsen van bestelorders binnen raamcontract.	Tot € 250.000	Tot € 100.000	Tot € 25.000	Tot € 10.000
Plaatsen van bestelorders van noodzakelijke goederen/ diensten volgens afgesproken richtlijnen.	Tot € 250.000	Tot € 50.000	Tot € 15.000	Tot € 5.000
Plaatsen van bestelorders voor het standaardassortiment bij geselecteerde leveranciers.	Tot € 250.000	Tot € 100.000	Tot € 25.000	Tot € 10.000
Beheren, adviseren en onderhouden van assortiment	X	X	X	X

Tabel 3 Bevoegdheden Inkoop

[144] Algemene bevoegdheidsregeling UMCG.
[145] Algemene bevoegdheidsregeling UMCG.

8 PRAKTIJKRESULTATEN

In dit hoofdstuk zijn de bevindingen weergegeven voortvloeiend uit de interviews met de controllers van de sectoren binnen het UMCG. Daarnaast zijn de opvattingen en verkregen informatie voortvloeiend uit gesprekken met UMCG medewerkers over het onderzoek meegenomen. Al deze mensen zijn gemakshalve gecategoriseerd onder het begrip respondenten. De resultaten van de afgenomen interviews en gesprekken zijn opgenomen in een aantal paragrafen waarin de bevindingen een antwoord geven op de praktijkgerichte deelvragen. Achtereenvolgens komen de volgende onderwerpen aan de orde: belangen UMCG (§ 8.1), compliance en implementatie EPV (§ 8.2), contracteren binnen het UMCG (§ 8.3) en tot slot infrastructuur contractbeheer sectoren/ afdelingen (§ 8.4).

Dit onderzoek heeft zich gericht op de situatie anno 2015 binnen de sectoren/ afdelingen van het UMCG, waar de situatie binnen de sectoren/ afdelingen nagenoeg overal hetzelfde was. Als er gesproken wordt van sectoren/ afdelingen wordt gedoeld op de sectoren/ afdelingen van A tot en met E.

8.1 BELANGEN UMCG

8.1.1 BELANGEN UMCG ALS ORGANISATIE

Het UMCG heeft als organisatie meerdere belangen in het kader van de EPV en het contractbeheer. Het UMCG heeft ten eerste het belang dat het moet en wil voldoen aan de wet- en regelgeving, zoals die wordt gesteld binnen de Europese Unie en Nederland. Immers, als het UMCG niet voldoet aan de wet- en regelgeving kunnen toezichthouders boetes uitschrijven op grond van niet-naleving van de wet- en regelgeving. Het tweede belang, het imago van het UMCG, hangt hiermee samen. Als het UMCG de EPV niet naleeft betekent dat het UMCG de privacy omtrent gegevensverwerkingen niet op orde heeft en niet voldoende waarborgt. Dit kan leiden tot negatieve publiciteit in de landelijke en regionale media, alsook op sociale media zoals Facebook en Twitter.

Naast de mogelijke negativiteit omtrent het imago als gevolg van niet-naleving wet- en regelgeving, is de andere kant van een goed imago, het belang van kwaliteit. Door het huidige contractbeheer af te zetten tegen het benodigde contractbeheer in het kader van de EPV, kan het UMCG handelingen veranderen in de werkwijzen en processen. Als het contractbeheer niet goed zou functioneren, kunnen derde partijen de professionaliteit van het UMCG in twijfel trekken. Daarnaast zou het UMCG met een slecht functionerend contractbeheer niet compliant zijn aan de EPV, gezien de EPV overzicht en inzicht in de gegevensverwerkingen vraagt. Voornoemde betekent dat er een goed contractbeheer moet zijn om dat te bewerkstelligen. Tot slot heeft het UMCG een financieel belang. Als er onvoldoende overzicht is van de contracten die worden gesloten binnen het UMCG, is er logischerwijze onvoldoende overzicht van de contracten die moeten worden beëindigd. Eventuele contracten die beëindigd moeten worden lopen daarom door, wat betekend dat de betalingsverplichtingen, mogelijk niet gering van aard, jegens de wederpartij(en) ook doorlopen. Voornoemde kan leiden tot financiële verspilling. Kortom, een ongunstige financiële situatie voor het UMCG.

8.1.2 BELANGEN SECTOREN/AFDELINGEN UMCG

De sectoren/ afdelingen hebben net als het UMCG als organisatie het belang dat ze moeten en willen voldoen aan de wet- en regelgeving, zoals die wordt gesteld binnen de Europese Unie en Nederland. Het tweede belang is het imago van de sectoren/ afdelingen binnen het UMCG. Als de sectoren/ afdelingen zaken niet goed op orde hebben krijgen ze een zogenaamde 'negatieve stempel' en worden de sectoren/ afdelingen mogelijk gekort in het kader van de financiën, waardoor projecten/ onderzoeken niet kunnen worden uitgevoerd. Het derde belang van de sectoren/ afdelingen is dat ze behoefte hebben aan duidelijkheid omtrent welke gegevens wel en niet mogen worden ingezien en verwerkt, anders gezegd een duidelijke bevoegdhedenregeling in het kader van de EPV. Op het moment is die bevoegdheid nog niet duidelijk afgestemd binnen het UMCG. Ten slotte is het vierde belang van de sectoren/ afdelingen

dat er duidelijkheid komt over de bevoegdheid om contracten te mogen tekenen. De tekenbevoegdheid is op het moment namelijk nog niet eenduidig duidelijk voor mogelijk veel medewerkers van UMCG.

8.2 Compliance en implementatie EPV

De respondenten gaven aan dat de EPV over het algemeen een erg onderbelicht onderwerp is binnen het UMCG, met name ten aanzien van het contractbeheer. Iedereen is op de hoogte dat er binnen een ziekenhuis streng toezicht moet worden gehouden op de verwerking van persoonsgegevens, maar het heeft nog geen dusdanige prioriteit dat het toezicht consequent wordt uitgevoerd. De sectoren/ afdelingen zijn daarom allen onbewust onbekwaam. De contractenadministratie en het toezicht/ naleving zijn bij de sectoren/ afdelingen veelal verschillend. Dit komt mogelijk doordat de sectoren vaak anders zijn georganiseerd. Bij de ene sector wordt het contractbeheer door de afdelingsmanagers gedaan en bij de andere sector door een medewerker vanuit een afdeling. Doordat de contracten door verschillende mensen worden beheerd, wordt de privacybescherming van gegevensverwerkingen mogelijk niet integraal geborgd. Op het moment is het UMCG daarom nog niet EPV-compliant. Dit is volgens de respondenten ook niet zo vreemd, gezien het een nieuwe verordening betreft.

8.2.1 Mogelijke oplossing

De respondenten gaven als mogelijke oplossing om compliance en implementatie EPV te bewerkstelligen, door het in eerste instantie op UMCG centraal niveau goed te regelen en daarnaast bewustwording te creëren bij de sectoren/ afdeling. Ten aanzien van het eerste punt moet er vanuit de Umc-staf informatie komen, wat kan worden gecommuniceerd aan de sectoren. De sectoren kunnen de desbetreffende informatie vervolgens communiceren aan de onderliggende afdelingen. De vraag wie binnen de sectoren de informatie moet communiceren aan de afdelingen ligt volgens de respondenten bij de kwaliteitsmanager en niet bij de controller. Met andere woorden: als eerste moet er UMCG centraal beleid zijn met betrekking tot het naleven en de implementatie van de EPV, waar de rest van de organisatie dan op kan anticiperen. Ten aanzien van het tweede punt, de bewustwording, werd aangegeven dat er behoefte is aan informatie vanuit de Privacy-werkorganisatie. Door de respondenten werd gedacht aan het houden van bijvoorbeeld een presentatie in de overleggen van controllers, afdelingsmanagers en afdelingshoofden. Kortom, er is behoefte aan een kernachtige voorlichting omtrent wat wel en niet mag in het kader van de EPV en de daaruit voorvloeiende gevolgen.

8.3 Contracteren binnen het UMCG

8.3.1 Derden

Contracten hebben in het ziekenhuiswezen vaak een sterke relatie met gegevensverwerkingen. Immers bij een gegevensverwerking door een derde partij hoort een overeenkomst waarin is vastgelegd welke afspraken er tussen het UMCG en de derde partij zijn gemaakt. De sectoren/ afdelingen van het UMCG sluiten naar behoefte contracten met derden in het kader van persoonsgegevensverwerkingen. Derden in dit kader zijn met name partijen als andere ziekenhuizen (bijvoorbeeld het Martini Ziekenhuis), zorgverzekeraars en leveranciers. Veelal is het wel zo dat als er bijvoorbeeld sprake is van samenwerkingsovereenkomsten, dat het via de Raad van Bestuur gaat. De sectoren/ afdelingen leggen dan wel het contact, maar zodra het gaat formaliseren wordt de Raad van Bestuur daarbij betrokken. In het kader van bijvoorbeeld de leveranciers kan gedacht worden aan de levering van bijvoorbeeld softwaresystemen waarin patiëntengegevens worden verwerkt.

Als de behoefte ontstaat tot contracteren van een derde, wordt de staf Juridische Zaken meestal niet betrokken bij de juridische toetsing van het contract. Dit is volgens de respondenten geen ideale situatie, gezien de juridische toets een belangrijk component is van het contracteren. Daarnaast zit de kennis omtrent rechtsgeldige contracten bij de staf Juridische Zaken, wat betekent dat bij een goede betrokkenheid van de staf Juridische Zaken er minder risico wordt gelopen ten tijde van het contracteren. Betrokkenheid van de staf Juridische Zaken wordt meestal pas tot stand gebracht als het fout dreigt te gaan of het al fout is gegaan. De afdeling Inkoop is volgens de respondenten altijd betrokken bij de afname van diensten of de aanschaf van informatiesystemen.

8.3.2 Soorten contracten

Binnen de sectoren/ afdelingen worden verschillende contracten gesloten, schriftelijk alsook mondeling. Meestal worden de contracten specifiek opgemaakt zodra er behoefte ontstaat om te contracteren. Er wordt echter ook vaak gebruikgemaakt van standaardcontracten, zoals bij detacheringsovereenkomsten. Daarnaast worden afspraken uit het verleden met bekende wederpartijen vaak geherformuleerd, met als uitgangspunt dat het toentertijd allemaal goed was geregeld. Hierdoor ontstaat geen behoefte om de nieuw te sluiten contracten met de 'bekende' wederpartij aan te passen of de onderhandelingen formeler in te richten. In de standaardmodelcontracten is vaak geen geheimhoudingsverklaring opgenomen. Voor een dergelijk bepaling is wel behoefte bij de respondenten. De privacybepaling kan dan in elk modelcontract standaard worden opgenomen ter bescherming van de privacy. Daarnaast benoemen de standaardcontracten ook niets over het wissen van gegevens van de betrokkene na beëdiging van het contract. Al met al voldoet de huidige situatie van de contracten niet voldoende aan de toekomstige EPV.

De contractvormen die voorkomen binnen de sectoren/ afdelingen zijn:
- contracten voor samenwerkingen i.h.k.v. zorg;
- contracten voor samenwerkingen i.h.k.v. opleiding;
- contracten voor samenwerkingen i.h.k.v. consulentschappen;
- overige samenwerkingen;
- contracten i.h.k.v. onderzoek;
- contracten met zorgverzekeraars;
- contracten i.h.k.v. arbeidsovereenkomsten en detachering.

8.4 Infrastructuur contractbeheer sectoren/ afdelingen

8.4.1 Huidige contractbeheer

Het UMCG begint in toenemende mate behoefte te krijgen aan een gestructureerde wijze van contractbeheer. Tot op heden heeft het contractbeheer nog niet prioriteit nummer één gehad en is het een onderontwikkeld aandachtsgebied. De EPV komt er echter binnen aanzienlijke tijd aan, waar het UMCG compliant aan moet en wil worden. Contractbeheer is in deze als kwaliteitsinstrument noodzakelijk om te voldoen aan de EPV. Het UMCG houdt zich in een zekere vorm bezig met contractbeheer, maar over het algemeen op ad-hoc basis en vaak op initiatief van een betrokken medewerker. Uit de beantwoording van de respondenten blijkt dat het er vaak even bij wordt gedaan of in de meeste gevallen zelfs helemaal niet. De wijze waarop het contractbeheer binnen de sectoren/ afdelingen van het UMCG plaatsvindt verschillen sterk. Bij sommige afdelingen liggen contracten her en der verborgen in mailboxen, bureaulades en kasten. Vaak is het ook zo dat er geen weet meer is van het contract, wat betekent dat de status van het contract niet duidelijk is. Dit kan leiden tot automatische verlening van contracten die helemaal niet meer relevant zijn voor de organisatie. Sectoren/ afdelingen die iets beter georganiseerd zijn, hebben het contractbeheer vastgelegd in Excel, Word, of in een digitaal systeem zoals Corsa. Contracten worden in dit geval wel vastgelegd. Dit blijkt uit de systemen en lijstjes waar de contracten in zijn geregistreerd. De mate van compliance, type gegevens, verantwoordelijken e.d. worden echter niet benoemd. Deze gegevens zijn wel noodzakelijk voor het overzicht en inzicht, wat de EPV eist. Bijvoorbeeld: in het digitale systeem Corsa zijn lopende en afgelopen contracten gearchiveerd. Maar over de contracten die stilzwijgend worden verlengd staat niets genoteerd binnen het systeem. De actuele status van contracten is daarom niet toetsbaar. Er kan dus niet worden geconcludeerd of het contract opgezegd, verlengd of vervangen moet worden door een ander contract. De toetsing betreffende toezicht en naleving wordt niet goed of helemaal niet gedaan. Dit heeft zeer waarschijnlijk te maken met het feit dat de verantwoordelijken niet duidelijk zijn binnen het UMCG.

8.4.2 2 Beheer verantwoordelijkheid

Binnen de sectoren/ afdelingen is het niet duidelijk wie er wel en niet bevoegd is om contracten te mogen tekenen. Daarnaast is het niet duidelijk wie eigenaar is van het contract. De verantwoordelijkheid verschilt volgens de respondenten mogelijk per contractonderwerp. De afdelingshoofden of de afdelingsmanagers zijn veelal belast met de bevoegdheid om te ondertekenen.

Binnen de sectoren/ afdelingen in bijvoorbeeld het domein onderzoek worden de contracten met een aan zekerheid grenzende waarschijnlijkheid beheerd door het domein zelf. Bij onderzoek sluiten de onderzoekers zelf hun contracten en worden de contracten hooguit getoetst op het financiële component en dus niet op het privacyaspect. De contracten omtrent bijvoorbeeld arbeidsovereenkomsten, detachering etc. liggen bij de afdeling P&O. Omtrent de overige contractvormen is de tekenbevoegdheid niet duidelijk bij veel medewerkers. De respondenten gaven wel aan dat er bevoegdheden zijn gerealiseerd in het kader van de algemene en specifieke bevoegdhedenregelingen binnen het UMCG. Dit heeft volgens de respondenten met name betrekking op de samenwerkingsovereenkomsten, waar de bevoegdheid bij de Raad van Bestuur ligt. Deze uitspraak komt overeen met beide bevoegdheidsregelingen van het UMCG. De contracten die worden gesloten met leveranciers liggen veelal bij Inkoop, waar een medewerker vanuit het Inkoop dat beheerd.

Geconcludeerd werd door de respondenten dat de tekenbevoegdheidsregeling bij mogelijk veel medewerkers niet eenduidig duidelijk is. Veelal worden de contracten getekend door de hoofden of managers vanuit de afdeling. Zijn de handtekeningen op de contracten door 'onbevoegden' wijsheid? Nee, absoluut niet. Mogelijk wordt de persoon (en niet het UMCG) die onbevoegd tekende aansprakelijk geacht voor bijvoorbeeld niet-naleving. Als de belangen groter worden, is er pas betrokkenheid van de Raad van Bestuur. Al met al hangt het af van de aard van het contract dat moet worden getekend en werd tot slot geconcludeerd dat de tekenbevoegdheidsregeling anno 2015 geen dusdanige prioriteit heeft binnen het UMCG.

8.4.3 Beheer contractvormen

De contractvormen binnen het UMCG bestaan uit verscheidende contractdocumenten zoals beschreven in paragraaf 8.3.2 en daarnaast uit mondelinge overeenkomsten en afspraken in brieven en e-mails. De laatst genoemde vormen zijn juridisch gezien ook contracten en worden veelvoudig gebruikt binnen het UMCG. Het nadeel van deze soorten contracten is dat ze erg lastig te beheren zijn. Dit, omdat er niet daadwerkelijk iets op papier wordt vastgelegd. Daarnaast is het aantonen van compliance in dit soort contracten een lastige activiteit. De controle op naleving van de mondelinge overeenkomsten wordt zo erg lastig, gezien deze niet goed kunnen worden beheerd.

8.4.4 Mogelijke oplossing

De voorkeur van de respondenten gaat uit naar een gecombineerd contractbeheer van centraal en decentraal. De voorkeur werd door de respondenten onderbouwd en luidt dat de contracten allen op centraal niveau moet worden geregistreerd en gearchiveerd, maar dat het toezicht en naleving bij decentraal (sectoren/ afdelingen) moet worden geplaatst. Dit, omdat decentraal de contracten sluit en daarom weet wat er speelt. Hierdoor kan er actief toezicht en naleving worden gehouden door een verantwoordelijke functionaris vanuit de desbetreffende sector/ afdeling.

De praktijkresultaten zijn nu geïnventariseerd en alle onderzoekspunten zijn hierin aan de orde gekomen. Nu kunnen de analyses geformuleerd worden. Allereerst volgt nog een korte uiteenzetting van het praktijkonderzoek en wordt afgerond met een korte conclusie.

9 KORTE UITEENZETTING PRAKTIJKONDERZOEK

Alvorens wordt overgegaan op hoofdstuk 10, is gekozen om het praktijkonderzoek kort uiteen te zetten. Dit komt de begrijpelijkheid van hoofdstuk 10 ten goede. Tot slot wordt dit hoofdstuk afgesloten met een conclusie.

9.1 RESULTATEN IN HET KORT

9.1.1 HUIDIGE BEVOEGDHEDENREGELING UMCG

In het kader van de sectorvorming zijn met ingang van 1 mei 2007 verantwoordelijkheden en de daarbij behorende bevoegdheden zoveel mogelijk op sectorniveau belegd. De bevoegdheden voor de sectordirecteuren zijn gemandateerd vanuit de Raad van Bestuur.

9.1.2 COMPLIANCE EN IMPLEMENTATIE EPV

De EPV is over het algemeen een erg onderbelicht onderwerp binnen het UMCG. De sectoren/ afdeling zijn ten aanzien van de EPV onbewust onbekwaam. De contractenadministratie en het toezicht/ naleving zijn bij de sectoren/ afdeling veelal verschillend. Dit komt mogelijk doordat de sectoren vaak anders zijn georganiseerd. Doordat de contracten door verschillende mensen worden beheerd, wordt de privacybescherming van gegevensverwerkingen mogelijk niet integraal geborgd. Op het moment is het UMCG daarom nog niet EPV-compliant. De respondenten gaven als mogelijk oplossing om compliance en implementatie EPV te bewerkstelligen, door het in eerste instantie op UMCG centraal niveau goed te regelen en daarnaast bewustwording te creëren bij de sectoren/ afdeling.

9.1.3 CONTRACTEREN BINNEN HET UMCG

De sectoren/ afdelingen van het UMCG sluiten naar behoefte contracten met derden in het kader van persoonsgegevensverwerkingen. Derden in dit kader zijn met name partijen als andere ziekenhuizen, zorgverzekeraars en leveranciers. Als de behoefte ontstaat tot contracteren van een derde, wordt de staf Juridische Zaken meestal niet betrok ken bij de juridische toetsing van het contract. Betrokkenheid van de staf Juridische Zaken wordt pas bewerkstelligd als het fout dreigt te gaan of het al fout is gegaan. De afdeling Inkoop is altijd betrokken bij de afname van diensten of de aanschaf van informatiesystemen. Binnen de sectoren/ afdelingen worden verschillende contracten gesloten, schriftelijk alsook mondeling. Meestal worden de contracten specifiek opgemaakt zodra er behoefte ontstaat om te contracteren. Daarnaast wordt ook veel gebruikgemaakt van standaardcontracten. Al met al is de huidige situatie van het contracteren binnen het UMCG niet EPV geborgd.

9.1.4 HUIDIGE CONTRACTBEHEER

Het UMCG houdt zich in een zekere vorm bezig met contractbeheer, maar over het algemeen op ad-hoc basis en vaak op initiatief van een betrokken medewerker. De wijze waarop het contractbeheer binnen de sectoren/ afdelingen van het UMCG plaatsvindt verschillen sterk. Bij sommige afdelingen liggen contracten her en der verborgen in mailboxen, bureaulades en kasten. Vaak is het ook zo dat er geen weet meer is van het contract, wat betekent dat de status van het contract niet duidelijk is.

9.1.5 VERANTWOORDELIJKHEID EN AUTORISATIE

Binnen de sectoren/ afdelingen is het niet duidelijk wie er bevoegd is om contracten te mogen tekenen. Daarnaast is het niet duidelijk wie eigenaar is van het contract. De contractvormen binnen het UMCG bestaan uit verscheidende contractdocumenten en daarnaast uit mondelinge overeenkomsten en afspraken in brieven en e-mails.

9.1.6 BELANGEN UMCG

Het UMCG heeft als organisatie de taak om te voldoen aan de wet- en regelgeving. Het imago van het UMCG hangt hiermee samen. Als het UMCG de EPV niet naleeft, betekent dat het UMCG de privacy omtrent gegevensverwerkingen niet op orde heeft en niet voldoende waarborgt. Aan de andere kant van een goed imago, staat het belang

van kwaliteit. Vanuit het UMCG is er behoefte aan een goed functionerend contractbeheer, dit ten aanzien van compliancy, alsook uit financieel belang.

9.1.7 Belangen sectoren/ afdelingen

De sectoren/ afdelingen hebben, net als het UMCG als organisatie, het belang dat zij moeten voldoen aan de wet- en regelgeving. Het imago van de sectoren/ afdelingen hangt hiermee samen. Bij een negatieve stempel kan dat de financiën schaden. Tot slot is er vanuit de sectoren/ afdelingen behoefte aan duidelijkheid omtrent de (teken)bevoegdheden en daarnaast verduidelijking omtrent welke gegevens zij wel en niet mogen inzien en verwerken.

9.2 Conclusie

Het UMCG is op dit moment niet EPV-compliant. Er is nog geen bewustwording en daarnaast is er geen goed functionerend contractbeheer binnen de sectoren/ afdelingen van het UMCG. De sectoren/ afdelingen willen wel graag veranderen om compliant te worden aan de EPV. Daarnaast is er behoefte aan een professioneel contractbeheer.

In het volgende hoofdstuk worden de analyses gehouden door de resultaten van het praktijkonderzoek te vergelijken met de theoretische inzichten omtrent de onderzoekspunten.

10 Analyse

10.1 Inleiding

In dit hoofdstuk volgt een uiteenzetting van analyses door de resultaten van het praktijkonderzoek te vergelijken met de theoretische inzichten omtrent de onderzoekspunten. De analyses hebben betrekking op compliance en implementatie EPV (§ 10.2), contractbeheer (§ 10.3), contracteren (§10.4) en tot slot autorisatie (§ 10.5). Op basis van de analyses is een eindconclusie geformuleerd, die is verwoord in hoofdstuk 11.

10.2 Analyse compliance en implementatie EPV

Uit de theorie met betrekking tot compliance en implementatie blijkt dat als een organisatie compliant wil worden aan nieuwe wet- en regelgeving er gebruik kan worden gemaakt van de compliancecyclus. De compliancecyclus is een methode om een bepaalde wet of regeling binnen een organisatie te implementeren aan de hand van een afzonderlijk project. In het kader van de EPV kan daarvoor de PDCA-cirkel worden gebruikt om de EPV te implementeren en compliancy te creëren. De omgevingsfactoren hebben een prominente rol om het compliancetraject te laten slagen. De cultuur binnen een organisatie is namelijk leidend voor het goed laten slagen van het compliancetraject. Het bestuur en het management van de verschillende bedrijfsonderdelen hebben een voorbeeldfunctie: goed voorbeeld doet volgen. Omgekeerd is het veelal ook aan de orde: slecht voorbeeld doet volgen. Commitment en de onvoorwaardelijke support van het bestuur is daarom voor het compliancetraject noodzakelijk. [146]

Uit de resultaten van de praktijk blijkt dat het UMCG als organisatie niet compliant is aan de EPV. Het betreft namelijk een nieuwe verordening met veel veranderingen. Het UMCG kan daar op het moment nog niet aan voldoen. De respondenten gaven aan dat de EPV op het moment nog een erg onderbelicht onderwerp is binnen het UMCG, waar nog niet veel over is gecommuniceerd. De respondenten gaven als mogelijke oplossing om compliance en implementatie EPV te bewerkstelligen, door het in eerste instantie op UMCG centraal niveau goed te regelen. Vanuit de Umc-staf moeten ze met informatie komen, wat kan worden gecommuniceerd aan de sectoren. De sectoren kunnen de desbetreffende informatie communiceren aan de onderliggende afdelingen. Kortom, als eerste moet er UMCG centraal beleid zijn met betrekking tot compliance en implementatie EPV, waar de rest van de organisatie dan op kan anticiperen. [147]

De analyse die hieruit voortvloeit, is dat het UMCG m.b.t. tot compliance en implementatie de juiste gedachtegang heeft. Een juiste gedachtegang is natuurlijk een eerste stap. Op het moment is de compliance echter nog niet goed binnen de sectoren/ afdelingen van het UMCG. Ten eerste omdat er nog geen bewustwording is omtrent de EPV en ten tweede wordt slecht gecommuniceerd over de EPV.

10.3 Analyse contractbeer binnen de sectoren/ afdelingen

Uit de theorie blijkt dat contractbeheer als doel heeft om de organisatie voldoende inzicht te verschaffen in (lopende) contracten en daarnaast de juiste contractuele afspraken en informatie verkrijgen door het voeren van een daarvoor bestemde administratie in een (centraal) contractenregister. Het contractenregister vormt een informatieverzameling van al die contracten en andere belangrijke gegevens die van toepassing zijn op de contracten, zoals het soort contract, leverancier, interne afnemer, data, status en soort product/ dienstverlening. Om een goed contractbeheer te bewerkstelligen is het noodzakelijk dat de informatie altijd up-to-date is en beschikbaar voor de betrokkenen en bevoegden. Door het voeren van een overzichtelijk contractbeheer wordt er een beheersbare situatie gecreëerd. Door het ontbreken van een centraal inzicht in de geldende contracten ontstaat er een onbeheersbare si-

[146] § 7.2.

[147] § 8.2.

tuatie. De onbeheersbare situatie heeft tot gevolg dat contracten zoek raken, oude contracten blijven in stand en zwerven door de organisatie heen, informatie uit geldende contracten blijven onbenut en contracten worden niet op tijd verlengd of beëindigd. Een disfunctionerend contractbeheer heeft daarom mogelijk (grote) financiële consequenties ten gevolge. Om goed toezicht en naleving te bewerkstelligen, is het erg zinvol om dat actief te bewaken. Er kan daarvoor een verantwoordelijk functionaris worden aangesteld zoals een contractenbeheerder en/of contractencoördinator. De verantwoordelijke functionaris moet controleren of de wederpartij zich aan de contractverplichtingen houdt en daarnaast is het wijsheid dat de functionaris de termijnen voor het uitvoeren van activiteiten die aflopen bewaakt.[148]

Uit de praktijk blijkt dat de sectoren/ afdelingen zich in een zekere vorm bezighouden met contractbeheer. Uit de beantwoording van de respondenten blijkt namelijk dat het contractbeer er vaak even bij wordt gedaan of in de meeste gevallen zelfs helemaal niet. De wijze waarop het contractbeheer binnen de sectoren/ afdelingen van het UMCG plaatsvindt verschillen sterk. Bij sommige afdelingen liggen contracten her en der verborgen in mailboxen, bureaulades en kasten. Sectoren/ afdelingen die iets beter georganiseerd zijn, hebben het contractbeheer vastgelegd in Excel, Word, of in een digitaal systeem. De toetsing betreffende toezicht en naleving wordt niet goed of helemaal niet gedaan. Dit heeft volgens de respondenten zeer waarschijnlijk te maken met het feit dat de verantwoordelijken niet duidelijk zijn binnen het UMCG.[149]

De analyse die hieruit voortvloeit is, dat er een versnipperd, geen proactief en geen goed functionerend contractbeheer is binnen de sectoren/ afdelingen van het UMCG.

10.4 Analyse contracteren binnen het UMCG

Uit de theorie blijkt dat om goede (EPF-proof) contracten te bewerkstelligen er een beoordeling door anderen dan de contractopstellers gewenst is. De contracten moeten namelijk juridisch worden getoetst door de Juridische afdeling van de organisatie. De juridische toetst moet worden uitgevoerd met inachtneming van de nieuwe wet- en regelgeving. Daarnaast moet het financieel verantwoord zijn. Tot slot is het wenselijk en in sommige gevallen noodzaak dat het af te sluiten contract in lijn met de strategie van de organisatie ligt. Standaardisatie van de contracten wordt ook geadviseerd in de theorie. Gezien deze contracten maar eenmaal juridisch behoeven te worden getoetst, wat tijdbesparing oplevert. Tijd wordt bespaard, gezien de Juridische afdeling van de organisatie zo niet elk nieuw te sluiten contract hoeft te toetsen. Hierdoor kan het proces waarschijnlijk worden versneld.[150]

Uit de resultaten van de praktijk blijkt dat op het moment de contracten niet EPV-proof zijn geborgd, waardoor het UMCG na de implementatietermijn (handhaving mogelijk per 01-01-2017) van de EPV in gebreke is. Het initiatief om contracten te sluiten ligt nu veelal bij de afdelingen. Waar nodig zoeken de afdelingen ondersteuning bij de staf Juridische Zaken, echter wordt dit veelal niet standaard gedaan. Daarnaast hebben de sectoren/ afdelingen niet de kennis en kunde om goede volledige contracten op te stellen. Naast specifiek opgestelde contracten, worden binnen de sectoren/ afdelingen ook vaak gebruikt van standaardcontracten. Deze standaardcontracten zijn op het moment volgens de respondenten niet EPV-proof.[151]

De analyse die hieruit voortvloeit is, dat er nog veel moet gebeuren om de contracten EPV-proof te maken. Op het moment wordt de kennis en kunde van de staf Juridische Zaken niet voldoende benut. Hierdoor worden de contracten niet juridisch getoetst wat betekent dat de contracten niet EPV-proof worden afgesloten.

10.5 Analyse autorisatie

Uit de theorie blijkt dat als de beoordeling vanuit de organisatie akkoord is en beide partijen akkoord zijn gegaan met de inhoud van het contract, er getekend kan worden. Contracten zijn vaak verschillend en bestaan daarnaast uit di-

[148] § 4.6, § 5.1, § 5.3.7, § 5.3.6, § 5.3.10 en § 5.4.
[149] § 8.4.
[150] § 5.3.3, § 5.3.5 en § 5.3.6.
[151] § 8.3.

verse smaken. Binnen het autorisatiebeleid moet daarom duidelijk naar voren komen, communicatie, wie bevoegd is om het contract te tekenen. Voornoemde kan volgens de theorie eenvoudig worden bewerkstelligd door het categoriseren van de contracten en de verschillende contractcategorieën koppelen aan een functionaris die bevoegd is om te tekenen en dit beleid eenduidig te communiceren aan de medewerkers van de organisatie. [152]

Uit de resultaten van de praktijk blijkt dat binnen het UMCG bij veel medewerkers de tekenbevoegdheid mogelijk niet duidelijkheid is. Uitzondering daarop is de samenwerkingsovereenkomst. Het is duidelijk dat bij die contracten de Raad van Bestuur tekenbevoegd is. Deze bevoegdheid staat vermeldt in de algemene bevoegdhedenregeling van het UMCG.[153]

De analyse die hieruit voortvloeit is, dat veel contracten mogelijk worden getekend door onbevoegden. Deze onbevoegden zijn dan aansprakelijk voor bijvoorbeeld de schade die voortvloeit uit wanprestatie. Binnen het UMCG is het autorisatiebeleid daarom nog niet eenduidig duidelijk bij veel medewerkers van de sectoren/ afdelingen.

De eindconclusie en de daaruit voortvloeiende aanbevelingen voor het UMCG zijn geformuleerd in hoofdstuk 11. Door middel van de conclusie en de aanbevelingen wordt een antwoord gegeven op de centrale onderzoeksvraag.

[152] § 5.3.6.
[153] § 8.4.2.

11 Conclusie en aanbevelingen

11.1 Inleiding

De informatie voortvloeiend uit de analyses van het literatuuronderzoek en het praktijkonderzoek hebben geleid tot een conclusie en aanbevelingen, die samen een antwoord op de centrale onderzoeksvraag geven. De centrale onderzoeksvraag van dit onderzoek luidt:

- *Op welke wijze kan er binnen de sectoren/afdelingen van het UMCG het contractbeheer worden ingericht, met de Europese Privacy Verordening als uitgangspunt en rekening houdend met de verschillende belangen van de sectoren/afdelingen binnen het UMCG?*

11.2 Conclusie

Met de komst van de EPV zijn organisaties genoodzaakt om de bedrijfsvoering op bepaalde punten aan te passen om compliant te worden aan de EPV. Het UMCG is één van de organisaties die graag compliant wil worden aan de EPV, welke vermoedelijk per 01-01-2017 wordt gehandhaafd. Hier moeten een aantal zaken voor veranderen, waaronder het contractbeheer. De EPV kan geïmplementeerd worden door het toepassen van de compliancecyclus. Om de compliancecyclus goed te realiseren zijn de omgevingsfactoren van belang. Commitment en de onvoorwaardelijke support van de Raad van Bestuur en de Umc-staf zijn daarom voor het compliancetraject van groot belang. Contractbeheer is één van de zaken die moet worden aangepast binnen het UMCG. Eén van de belangrijkste eisen van de EPV is het hebben van overzicht en inzicht in de gegevensverwerkingen. Contractbeheer kan worden gebruikt als instrument om dat te bewerkstelligen. De conclusie van het onderzoek is dat op het moment geen goed genoeg functionerend contractbeheer is binnen het UMCG om te kunnen voldoen aan de EPV. Dit kan mogelijk verklaard worden door de huidige manier van contractenadministratie en onduidelijke verantwoordlijkheden. Daarnaast wordt op het moment niet consequent gebruikgemaakt van de kennis en kunde van de staf Juridische Zaken om toekomstige contracten EPV-proof af te sluiten. Tot slot is binnen het UMCG bij mogelijk veel medewerkers niet duidelijk wie tekenbevoegd is. Dit kan leiden tot contracten die onbevoegd worden ondertekend. Hierdoor kan de onbevoegde ondertekenaar, en niet het UMCG, aansprakelijk worden gesteld. Ondanks de strenge eisen die de EPV stelt, biedt de verordening kansen voor het UMCG om te veranderen en mogelijkheden om de huidige manier van contractbeheer anders in te richten/ te verbeteren. Bij de implementatie van de EPV binnen het UMCG moeten de belangen van het UMCG als organisatie, alsook de belangen van de sectoren/ afdelingen worden meegenomen. Deze belangen zijn geïnventariseerd en luiden:

- Het UMCG heeft als organisatie de taak om te voldoen aan de wet- en regelgeving. Het imago van het UMCG hangt hiermee samen. Als het UMCG de EPV niet naleeft, betekent dat het UMCG de privacy omtrent gegevensverwerkingen niet op orde heeft en niet voldoende waarborgt. Aan de andere kant van een goed imago, staat het belang van kwaliteit. Vanuit het UMCG is er behoefte aan een goed functionerend contractbeheer, dit ten aanzien van compliancy, alsook uit financieel belang.
- De sectoren/ afdelingen hebben, net als het UMCG als organisatie, het belang dat ze moeten voldoen aan de wet- en regelgeving. Het imago van de sectoren/ afdelingen hangt hiermee samen. Bij een negatieve stempel kan dat de financiën schaden. Daarnaast is er vanuit de sectoren/ afdelingen behoefte aan duidelijkheid omtrent de (teken)bevoegdheden en behoefte aan verduidelijking omtrent welke gegevens zij wel en niet mogen inzien en verwerken.

11.3 Aanbevelingen

Het UMCG wordt aanbevolen om met de komst van de EPV een aantal zaken te veranderen, om compliant te worden aan de EPV. Zoals aangegeven is het opnieuw inrichten van het contractbeheer daar één onderdeel van. De aanbevelingen om het UMCG aan de verordening te laten voldoen, met inachtneming van de belangen van het UMCG en haar sectoren/ afdelingen luiden:

1. Om EPV compliancy te realiseren binnen het UMCG, is het eerst noodzakelijk om privacybewustwording ten aanzien van gegevensverwerking te creëren. De sectoren/ afdelingen zijn op het moment allen onbewust onbekwaam. De Privacy-werkorganisatie kan bewustwording creëren door het gegeven van voorlichtingen in overleggen die worden gehouden door controllers, afdelingshoofden, managers etc. De voorlichting kan onderwerpen bevatten zoals wat mag wel en wat mag niet worden verwerkt ten aanzien van gegevens, wie is bevoegd tot gegevens inzage, welke EPV veranderingen vinden er plaats? etc. Daarnaast dienen beleidsontwikkelingen omtrent de EPV te worden gepubliceerd op het UMCG intranet en directe betrokkenen dienen op de hoogte worden gesteld door middel van e-mail.

2. De wijzigingen van de EPV kunnen met behulp van de compliancecyclus binnen het UMCG worden geïmplementeerd en worden toegepast binnen het contractbeheer. De stappen die hiervoor gevolgd kunnen worden staan omgeschreven in hoofdstuk 6.

3. Op het moment is er geen goed functionerend contractbeheer aanwezig binnen de sectoren/ afdelingen van het UMCG. Dit kan leiden tot ongunstige (financiële) situaties. Allereerst moet er een inventarisatie van alle contracten binnen de sectoren/ afdelingen worden gehouden. Immers, zonder een goed overzicht van alle contracten kan er geen contractbeheer worden gecreëerd en kan niet worden voldaan aan de EPV. Er moet daarom een goede communicatie te worden bewerkstelligd met de sectoren en met alle afdelingen die onder de sectoren hangen. Het creëren van bewustwording is hierin een prioriteit om de sectoren/ afdelingen in te laten zien dat iedereen moet bijdragen aan een goed werkende en professionele organisatie.

4. Om professioneel contractbeheer te realiseren wordt aanbevolen goed beleid te schrijven en de 14 fasen van het contractbeheerproces in acht te nemen. Deze 14 fasen staan uitgelegd in hoofdstuk 5. Het UMCG kan zelf invullen in hoeverre en op welke wijze de verschillende fasen worden uitgevoerd. Het beschreven contractbeheerproces kan daarom worden geïnterpreteerd als een kader waarbinnen het contractbeheer van het UMCG kan worden gerealiseerd. Daarnaast moet worden nagedacht welk systeem het UMCG bruikbaar acht. De capaciteit en eenvoud van zo'n digitaal systeem staat voorop. Aanbevolen wordt om een centraal contractbeheer in te richten. Dit komt de werkbaarheid ten goede en biedt een eenduidig overzicht waarin alles is opgenomen. Er kan worden overwogen om het toezicht en naleving decentraal te plaatsen. Ondanks de keuze centraal, decentraal of een combinatie van beide, het contractregister moet binnen het UMCG altijd actief up-to-date worden gehouden door de betrokken medewerkers.

5. Het contractbeheerbeleid moet actief worden nageleefd door de medewerkers van het UMCG. Dit is van groot belang om het project 'implementatie contractbeheer' te laten slagen. Zonder naleving is het project namelijk gedoemd te mislukken. Kortom, commitment van de Raad van Bestuur, UMC-staf en alle sectoren/ afdelingen is uitzonderlijk belangrijk. Dit is ook meteen het grootste risico en daarbij de grootste uitdaging van het UMCG.

6. Om per 1 september 2015 contracten EPV-proof af te sluiten wordt aanbevolen om een eenvoudige juridische checklist op te laten maken door de staf Juridische Zaken en/of de Privacy-werkorganisatie. De checklist moet zo worden opgemaakt dat de checklist ondubbelzinnig en eenduidig kan worden geïnterpreteerd door de betrokkenen. Gedacht kan worden aan het ontwikkelen van een format contract invoer formulier, waarin wordt uitlegt wat er wordt vastgelegd per contract ten aanzien van rechtsgeldigheid. Als deze activiteiten actief worden opgepakt ten aanzien van nieuw, opnieuw te sluiten contracten, kan dit proces snel en actief in werking worden gezet. De checklist kan bijvoorbeeld al worden gebruikt als een derde met een (concept)contract komt. Daarnaast kan de checklist worden meegenomen in de onderhandelingsfase om te checken of alle componenten worden meegenomen. Desalniettemin moet de staf Juridische Zaken altijd worden benaderd voor een juridische toetsing, de checklist kan het contracteertraject waarschijnlijk alleen versnellen.

7. Contracten die compliant zijn aan de EPV kunnen worden gerealiseerd door een goede samenwerking tussen de sectoren/ afdelingen en de staf Juridische Zaken. Op het moment wordt namelijk niet consequent gebruikgemaakt van de kennis en kunde van de staf Juridische Zaken. Het wordt daarom geadviseerd om een formeel protocol te creëren wanneer en hoe de controllers, afdelingshoofden en afdelingsmanagers in het kader van contracteren, contact dienen te zoeken met de staf Juridische Zaken. Bijvoorbeeld: als er contact wordt gelegd met een derde, om te contracteren, moet dit worden gemeld aan de staf Juridische Zaken. Met de staf Juridische Zaken kan dan worden overlegd of verdere hulp nodig is of dat kan worden overgegaan tot de onderhandelingsfase. De staf Juridische Zaken moet echter wel altijd een juridische toets te doen, tenzij er sprake is van een standaard EPV-proof contract. In het geval er sprake is van een groot/ complex contract kan worden afgesproken dat er actief contact worden gehouden tussen de sector/ afdelingen en de staf Juridische Zaken omtrent de stand van zaken. Dit om (financiële) risico's tijdig te signaleren en te anticiperen.

8. Binnen de sectoren/ afdelingen wordt vaak gewerkt met eenzelfde soort contract per onderwerp. Op het moment worden daar vaak standaardcontracten voor gebruikt. Deze voldoen echter niet aan de EPV. De standaardcontracten moeten daarom worden herzien, zodat ze voldoen aan de EPV. Het werken met standaardcontracten werkt namelijk tijdbesparend. Het werkt tijdbesparend gezien de verschillende standaardcontracten (eenmalig) EPV-proof worden opgesteld door de staf Juridisch Zaken. De standaardcontracten kunnen dan in alle algemene situaties bruikbaar worden geacht. Als er zich bijzondere omstandigheden voordoen, moet dit worden gecommuniceerd aan de staf Juridische Zaken. De staf Juridische Zaken kan dan beoordelen of het standaardcontract nog steeds van toepassing is, of dat er wijzigingen dienen plaats te vinden.

9. Binnen het UMCG is bij mogelijk veel medewerkers niet duidelijk wie tekenbevoegd is. Dit kan leiden tot contracten die onbevoegd worden ondertekend. Hierdoor kan de onbevoegde ondertekenaar, en niet het UMCG, aansprakelijk worden gesteld voor bijvoorbeeld niet-naleving. Om dit te voorkomen moet nadrukkelijk worden benadrukt bij de controllers, afdelingshoofden en afdelingsmanagers etc. binnen de sectoren/ afdelingen, dat de huidige situatie van contractondertekening niet meer kan. De huidige algemene- en specifieke bevoegdhedenregeling geven duidelijk aan wie wel en wie niet mag tekenen. Dit is voor de sectoren/ afdelingen uiteengezet in hoofdstuk 7. Kortom, de bevoegdhedenregeling moet duidelijk en eenduidig worden gecommuniceerd binnen het UMCG.

10. Naast contractbeheer wordt aanbevolen om contractmanagement in te richten. Dit om het contractbeheer te borgen. In nauwe samenwerking met de disciplines: de staf Financiën & Control, de staf Juridische Zaken en Inkoop kan een goed contractmanagementplan worden opgezet. In het plan kan worden beschreven hoe de verkregen input, getekende contracten en wijzigingen hierop eenduidig kunnen worden vastgelegd, beheerd en bewaakt. De samenwerking tussen de verschillende disciplines zal mogelijk leiden tot betere contractbeheersing.

11. Tot slot wordt aanbevolen om vervolgonderzoek te houden dat zich richt op de situatie binnen alle afdelingen van de sectoren A tot en met F. Dit, omdat sector F en de afdelingen binnen de sectoren A tot en met E niet diepgaand zijn onderzocht en geanalyseerd. Vervolgonderzoek wordt aanbevolen om een goed breed functionerend contractbeheer te bewerkstelligen binnen het UMCG. Immers de afdelingen sluiten met een aan zekerheid grenzende waarschijnlijk de meeste contracten.

Einde onderzoek

12 LITERATUURLIJST

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

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

Borking
J. Borking, '*Privacy by design en 'data protection by default'.* n: Privacy en Compliance – 03-04/2012.

Bouman
V. Bouman, 'Privacy beter beschermd onder Europese privacyverordening' Wieringa Advocaten 3 december 2014,www.wieringa-advocaten.nl (zoek op Europese privacy, weblog, Victor Bouman 03/12/2014), geraadpleegd op 17 februari 2015.

Brugman & R.J. Watson
G.J. Brugman & R.J. Watson, 'De nieuwe privacy verordening, *De Hypotheekadviseurs 2013,* p.47.

CBP
CBP, *informatie delen in samenwerkingsverbanden, nummer 31A, februari 2012.*

CBP
CBP, *Toegang tot digitale patiëntendossiers binnen zorginstellingen,* juni 2013.

DDMA
DDMA, 'Privacy Europa', 12 februari 2015, www.ddma.nl (zoek op Juridisch loket, dossiers, privacy Europa).

Duthler & Biesheuvel
A.W. Duthler & A.J. Biesheuvel, *Het Europese privacyrecht in beweging,* Deventer: Uitgeverij Kluwer 2013.

Hijl & Van der Meer
V.S.M. Hijl & D. Van der Meer, *Contractbeheer: Theorie in praktijk*, Heerde: Mercante Publishing 2002.

Hustinx
P.J. Hustinx, *'Begrip bewerker', CBP,* 14 mei 2002.

De Jong
J.P. de Jong, Regelmaat, *De Algemene verordening gegevensbescherming. De rechtsopvolger van de Wbp,* Boom Juridische Uitgever: 2015

Knoester
T. Knoester, *Management in de praktijk,* Houten: Bohn Stafleu van Loghum, 2005.

KNMG
Nieuwe Europese privacyregels in aantocht', KNMG 23 mei 2014, www.knmg.artsennet.nl (zoek op Europese privacyregels), geraadpleegd op 16 februari 2015.

Kranenborg & Verhey
H.R. Kranenborg & L.F.M. Verhey, *Wet bescherming persoonsgegevens in Europees perspectief,* Deventer: Kluwer 2011.

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

NPPP
Publicatie NPPP, *Contractbeheer en contractmanagement*, juni 2004.

NVZ
Privacy' NVZ, www.nvz-ziekenhuizen.nl (zoek op Europese privacyregels).

Overkleeft-Verbrug
De juridische evaluatie: G. Overkleeft-Verburg, *De Wet persoonsregistratie. Norm, toepassing en evaluatie*, Zwolle 1995 en de sociaal-wetenschappelijke evaluatie: J.E.J. Prins e.a., *In het licht van de Wet persoonsregistratie: Zon, Maan of Ster?*, Alpen a/d Rijn 1995.

Privacy-werkorganisatie
Rapport Privacy-werkorganisatie 'Implementatie EPV' versie 2.0, 2015.

Rijksoverheid
'Persoonsgegevens' Rijksoverheid, www.rijksoverheid.nl (zoek op 'persoonsgegevens'.

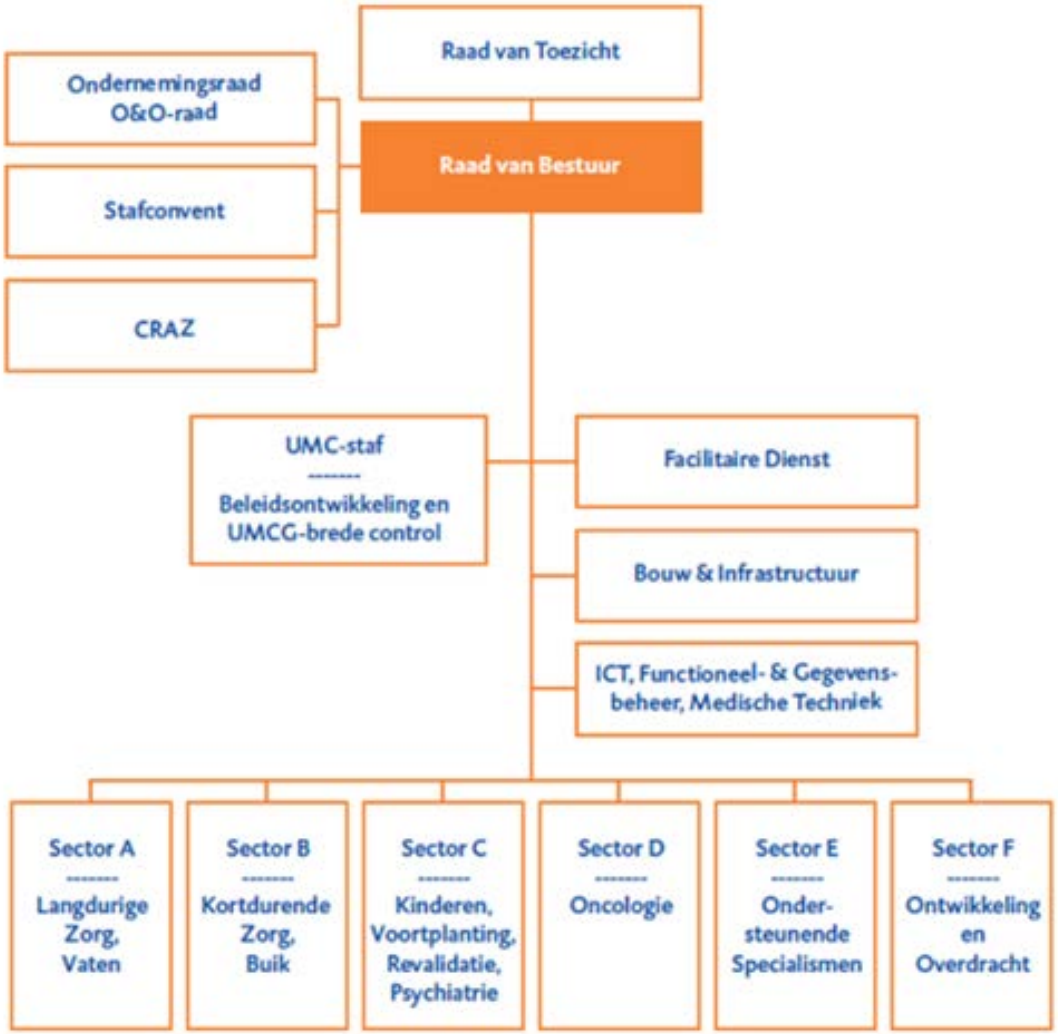
Tiggelen
J. Van Tiggelen, 'Archiveren', *Handboek Administratie,* oktober 1993. pp. A5570.

Van Schaaijk
G.A.F.M. van Schaaijk, *Praktijkgericht juridisch onderzoek*, Den Haag: Boom juridische uitgevers, 2011.

V&VN
V&VN Ambulancezorg, Ambulancezorg Nederland en Nederlandse Vereniging van Medische Managers Ambulancezorg, *Beroepsgeheim binnen de ambulancezorg; achtergrondnotitie en richtlijn.* Versie 2.0, augustus 2009.

Verschuren & Doorewaard
P. Verschuren & H. Doorewaard, *Het ontwerpen van een onderzoek*, Den Haag: Boom Lemma Uitgevers, 2007.

BIJLAGE 1 ORGANOGRAM UMCG



BIJLAGE 2 INTERVIEWVRAGEN

Algemeen

1. Wat is uw functie?

2. Hoe lang werkt u al in deze functie?

3. Bent u op de hoogte van de Europese Privacy Verordening en haar veranderingen?

Vragen m.b.t. contracten

1. Worden er binnen uw sector contracten met het oog op gegevensverwerkingen met externe derden gesloten, respectievelijk worden er onderhandelingen met derden gevoerd die tot contracten kunnen leiden?

2. Wie zijn die derden (naam en doel)?

3. Wat voor soort contracten worden er binnen de sector afgesloten?

4. Wat is het doel van die contracten (met het oog op de gegevensverwerking/ privacy)?

5. Wie is verantwoordelijk voor de contracten?

6. Is de sector/ afdelingen gemandateerd om zelf contracten met derden in het kader van persoonsgegevensverwerking te ondertekenen?

7. Gebruikt de sector standaardcontracten?
   a. Ja: Hoe zien die contracten eruit?
   b. Nee: Wat is daarvan de reden? Hoe komt zo'n contract tot stand? Wie doet in zo'n geval de juridische toets?

8. Is Inkoop bij afname van diensten of aanschaf van informatiesystemen betrokken?
   a. Is de staf Juridische zaken bij het contracteren betrokken? (juridische toets)

Vragen m.b.t contractbeheer

1. Wat is de huidige infrastructuur van het contractbeheer binnen de sector/afdelingen van het UMCG?
   a. Hoe worden de contracten geadministreerd?
   b. Geldt die administratie zo voor alle contracten?

2. Kunnen de contracten door alle medewerkers van het UMCG worden geraadpleegd/verzameld?

3. Welke functionaris zorgt er binnen uw sector/ afdelingen voor dat contracten worden nagekomen en op de juiste wijze worden uitgevoerd?

4. Hoe wordt er voor gezorgd dat contracten worden nagekomen en op de juiste wijze worden uitgevoerd?

Vragen m.b.t. de belangen

1. Wat zijn de belangen van de sector/afdelingen met betrekking tot een goede implementatie van de Europese Privacy Verordening?

2. Heeft u een idee hoe de sector kan voldoen aan de Europese Privacy Verordening?

3. Wat zijn, volgens u, de risico's binnen uw sector m.b.t. de privacywetgeving in contracten?
   a. Hoe zou u binnen de sector het bewustzijn rondom privacy kunnen verbeteren?
   b. Heeft u een idee hoe de sector ervoor kan zorgen dat alle nieuw te sluiten contracten EPV-compliant zijn?

4. Heeft u een idee hoe het contractbeheer idealiter kan functioneren?
   a. Wat zijn uw ideeën over goed werkend contractbeheer binnen het UMCG?

Gegevens		Beheer	
'mag het?'		*'hoe ga je er mee om?'*	
Rechtmatig verkregen gegevens - grondslagen voor rechtmatige verwerking: Ondubbelzinnige toestemming, noodzakelijk voor uitvoeren overeenkomst, wettelijke plicht, bescherming vitale belangen, taak van algemeen belang, gerechtvaardigd belang. Laatste grond geldt niet langer voor overheid.	6 8	***Implementatie en documentatie*** Organisaties moeten o.a. analyseren welke verwerkingen worden uitgevoerd door henzelf of hun leveranciers, welke soorten gegevens het betreft, voor welke doeleinden zij dit doen en welke beveiligingsmaatregelen getroffen zijn.	5, 22
Beginselen van toepassing op verwerking van persoonsgegevens: Rechtmatigheid, eerlijkheid en transparantie, doelbinding, minimale gegevensverwerking en opslag, juistheid, doeltreffendheid, integriteit en verantwoordingsplicht.	5 6-11	***Checken, bekijken en sluiten bewerkersovereenkomsten*** Bewerkersovereenkomsten met leveranciers of afnemers zijn nodig in het geval persoonsgegevens worden verwerkt. Bewerkersovereenkomsten moeten onder andere gedetailleerde informatie over de beveiligingsmaatregelen bevatten.	26, 77 14
Aantoonbare toestemming voor bepaalde doeleinden De bewijslast ligt bij de organisatie aan wie toestemming is verleend. Betrokkenen moeten deze toestemming te allen tijden eenvoudig kunnen intrekken. Bepalingen die niet	7 -	***Risicoanalyses en controlecycli*** Voor nieuwe en bestaande diensten moet een risico analyse worden uitgevoerd. Deze moet jaarlijks worden gecontroleerd/herhaald. Voor risicovolle diensten moet tweejaarlijks een 'impact assessment' worden uitgevoerd.	22/32a/32bis/33/33bis -

aan de regels voldoen zijn nietig.			
Doorgifte van persoonsgegevens Doorgifte buiten EU is slechts onder voorwaarden toegestaan. Multinationals kunnen bindende bedrijfsvoorschriften opstellen en door de nationale toezichthouder laten goedkeuren.	41-43 76-78	***Informatiebeveiliging*** Organisaties moeten informatie met passende technische en organisatorische maatregelen beveiligen.	22/30/33 23
Bijzondere persoonsgegevens (o.a. etniciteit, gezondheid, seksuele voorkeuren) Het verwerken van bijzondere persoonsgegevens is niet toegestaan of er gelden strikte voorwaarden.	9 16	***Beheer van toestemming en rechten van betrokkenen*** Systemen en processen voor rechten van betrokkenen zullen moeten worden ingericht en beheerd.	7/19 -
Extra bescherming voor kinderen onder de 13 jaar Verwerking van persoonsgegevens van kinderen jonger dan 13 jaar is alleen toegestaan na toestemming van een ouder of wettelijk vertegenwoordiger. Organisaties moeten zich redelijk inspannen om de toestemming te controleren.	8 -	***Dataportabiliteit*** Betrokkenen hebben het recht op een kopie van hun (persoons)gegevens in een elektronisch en bruikbaar formaat.	15 -
Profilering ('profiling') Profilering met juridische gevolgen is slechts onder voorwaarden toegestaan. Profilering met aanzienlijke gevolgen voor betrokkenen moet gebaseerd zijn op menselijke beoordeling en een uitleg van het besluit bevatten. Profilering op basis van pseudonieme gegevens is toegestaan.	20	***Aannemen beleid, implementeren technische en organisatorische maatregelen*** Organisaties moeten beleid opstellen en aantoonbaar technische en organisatorische maatregelen nemen om er voor te zorgen dat persoonsgegevens transparant en in overeenstemming met de regels worden verwerkt.	22/30/32a

Uitzondering voor bepaalde doelen Historische, statistische of wetenschappelijke doeleinden zijn uitgezonderd alsmede sociale zekerheid, religieuze organisaties, medewerkers en gezondheid.	5/42 /81/82 17- 23	***Bewaartermijn*** Beperk de opslagperiode en verwijder of archiveer (indien toegestaan) gegevens tijdig.	5/83a 10
Organisatie		**Communicatie**	
'hoe richt je de organisatie en processen in?'		*'hoe communiceer je erover?'*	
Functionaris voor de gegevensbescherming / data protection officer Organisaties moeten een functionaris voor de gegevensbescherming aanstellen. De functionaris rapporteert aan de directie.	35 62	***Duidelijke en begrijpelijke communicatie over persoonsgegevens*** Informatie en communicatie moeten in een begrijpelijke vorm en in duidelijke (gewone) taal zijn opgesteld, zeker als deze zich richt tot kinderen.	7/8/14/ 15/19
Rechten van betrokkenen (inzage, correctie, verwijderen, compensatie, bezwaar) Implementeer processen voor het uitoefenen van rechten. Betrokkenen mogen informatie opvragen over doel, bewaartermijn en logica achter de verwerking en mogen bezwaar maken tegen profilering.	15/22 35- 42	***Privacy beleid en gestandaardiseerd formulier*** Het privacy beleid moeten rechten van betrokkenen bevatten en beknopt, transparant en gemakkelijk toegankelijk zijn. Bij het verzamelen van persoonsgegevens moet een standaard formulier met door de EU vastgestelde iconen getoond worden.	11/13a/ A1 -
Meldplicht datalekken Implementeer processen voor het melden van datalekken.	31/32 -	***Melden datalekken bij toezichthouder en betrokkenen*** Datalekken moeten binnen 72 uur aan de toezichthouder gemeld worden en in sommige gevallen is directe melding aan de betrokkene vereist.	31/32 -
Getrainde medewerkers, een privacybewuste organisatie Om de risico's te minimaliseren moeten organisaties en	5/22 /26 -	***Contactgegevens functionaris voor de gegevensbescherming (FG)***	35 63

hun medewerkers bewust zijn van de belangrijkste elementen van de regelgeving.		Contactgegevens van de FG moeten worden gepubliceerd en betrokkenen moeten contact op kunnen nemen om hun rechten uit te oefenen.	
Privacy relevant voor ontwikkeling van producten en diensten (privacy by design/default) Weeg privacyaspecten mee bij het ontwikkelen van nieuwe producten en diensten. 'Privacy by design' is een voorwaarde bij openbare aanbestedingen.	23 -	***Communicatie met de toezichthouder*** De toezichthouder mag documenten en gegevens opvragen en heeft de bevoegdheid om toegang te krijgen tot alle persoonsgegevens en de locaties waar deze zijn opgeslagen.	29/53 60
Certificering Organisaties kunnen EU breed gecertificeerd worden door de nationale toezichthouder. Na certificering ('privacy seal') worden boetes alleen opgelegd in het geval van opzet of grove nalatigheid door de organisatie.	39/79 -	***Bezwaar tegen profilering*** Betrokkenen moeten op een uiterst zichtbare manier worden geïnformeerd over de mogelijkheid om bezwaar te maken tegen profilering.	20 -
Toezicht De toezichthouder in het land van de feitelijke hoofdvestiging van de organisatie zal verantwoordelijk zijn voor het toezicht.	54a -	***Jaarverslag*** Het jaarverslag of een andere reguliere zakelijke rapportage moet een korte beschrijving bevatten van het beleid en de maatregelen die zijn genomen.	22

154

[154] Privacy Company, http://www.privacycompany.eu (zoek op docs, overzicht AVG)

BIJLAGE 4 VEREISTEN BEWERKERS/ VERWERKERSOVEREENKOMST

Wettelijke eisen	Wbp	EPV
Verwerking kan slechts in opdracht van de verantwoordelijk.	X	X
Afspraken omtrent verzoeken van betrokkenen dienen te worden opgenomen.	X	X
Persoonsgegevens zijn voldoende beveiligd (bijv. NEN7510)	X	X
De verwerker biedt voldoende waarborging ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen.	X	X
De verantwoordelijke ziet toe op de naleving van de technische en organisatorische beveiligingsmaatregelen.	X	X
De verwerker moet de beveiliging aantonen m.b.v. gedragscodes of certificeringsmechanismen.		X
Meldplicht van datalekken aan de verantwoordelijke.		X
Geheimhouding/ vertrouwelijkheid.		X
Na beëindigen van de overeenkomst moet de verwerker alle resultaten teruggeven en kopieën verwijderen.		X
De verwerker mag niet zonder toestemming een andere verwerker in dienst nemen, ten anders is bepaalde tussen partijen.		X

BIJLAGE 5 FUNCTIE WERKZAAMHEDEN

Contractenbeheerder: voldoen aan standaardisatie-eisen van de contractencoördinator, verantwoordelijk voor onderstaande activiteiten. Procesgebonden activiteiten (PG) waar voordelig decentraliseren en standaardiseren.	**Contractencoördinator:** verantwoordelijk voor de contractgroepoverstijgende activiteiten. Dit betekent dat hij die of centraal moet (laten) uitvoeren, of sterk moet standaardiseren (alleen procesgebonden activiteiten (PG))
Registratie van decentrale gegevens (PG)	Laten beoordelen (PG)
Genereren/distribueren van informatie (PG)	Laten autoriseren (PG)
Bewaking van uitvoering/beëindiging (PG)	Archiveren (PG)
Inrichten van decentrale registers (PE)	Registreren centrale gegevens (PG)
Opstellen van standaardinhoudselementen en afspraken in specificaties (PE)	Laten opstellen van autorisatie- en beoordelingsbeleid. (PE)
Opstellen van eisen aan informatie voor wederpartijselectie (PE)	Opstellen van een beleid van toegankelijkheid informatie (PE)
Opstellen van standaardeisen voor selecteren wederpartijen (PE)	Laten uitvoeren van volledigheidcontroles (PE)
Opstellen van standaarddocumenten om reacties aan te vragen (PE)	Inrichten/opschonen van centrale registers en archieven (PE)
Opstellen van standaardinhoud van contracten (PE)	Coördinatie van het contractbeheerproces (coördinatie van de decentrale activiteiten, (laten) opstellen van procedures, borging van procedures) (PE)
Opstellen van standaardvoorwaarden (PE)	
Opstellen van standaardlay-out per contractgroep (PE)	

(PG) = procesgebonden activiteiten: voor elk contract uit te voeren.
(PE) = periodieke activiteiten: eenmalig of periodiek voor meerdere contracten.[126]

BIJLAGE 6 NORMENKADER

Nr. norm	*Voorschrift*	*Bron voorschrift (wet-regelgeving)*	*Toelichting*	*Bedrijfsonderdeel/-proces*	*Nr.beheersmaatregel*	*Beheersmaatregel*

BIJLAGE 7 RISICOMATRIX

Voorschrift	Bedrijfsonderdeel/-proces	Kans	Impact	Risico	Risicocategorie (alternatief)	Prioriteit	Toelichting

Kans K =klein; M = middelgroot; G = groot
Hoe groot is de kans dat niet wordt nageleefd?

Impact K =klein; M = middelgroot; G = groot
Gevolgen van niet-naleving voor de organisatie.

Risico ZK = zeer klein; K =klein; M = middelgroot; G = groot; ZG = zeer groot
Inschatting van het risico gezien kans en impact

Risicocategorie *3 = laag; 2 = middel; 1 = hoog*
Alternatief: een indeling in risicocategorieën is ook mogelijk.

Prioriteit: L = laag; M = middel; H = hoog
Prioritering implementatie beheersmaatregel(en). [1][2]