

2014

Privacybescherming van dak- en thuislozen

N. van Meel

Stichting maatschappelijke opvang

Traverse

7-1-2014

Privacybescherming van dak- en thuislozen

Stageplaats:

Stichting maatschappelijke opvang
Traverse, afdeling Beleid

Adres:

Reitse Hoevenstraat 6
Postbus 1314
5004 BH Tilburg
Tel. 013 - 464 50 99
Fax. 013 - 468 20 32

Begeleiding:

Afstudeermentor: Jose Buitendijk

1^e docent: J. pop

2^e docent: B. Kratsborn

Inhoudsopgave

Samenvatting	3
Lijst van afkortingen	5
Begrippenlijst Wbp.....	6
Hoofdstuk 1. Inleiding.....	7
1. Inleiding.....	7
1.1 Probleembeschrijving	7
1.2 Doelstelling.....	8
1.3 Vraagstelling	8
1.4 Onderzoeksmethodiek	8
1.5 Opbouw van het rapport	9
Hoofdstuk 2. Toegang digitaal cliëntdossier.....	10
2.1 Het digitaal cliëntdossier	10
2.2 Het beleid met betrekking tot de toegang tot digitale cliëntdossiers	10
2.3 De praktijk met betrekking tot de toegang tot digitale cliëntdossiers	11
2.3.1 De toegang	11
2.3.2 Logging.....	12
2.4 Ten slot.....	12
Hoofdstuk 3. Het delen van cliëntgegevens	13
3.1 Contacten	13
3.2 De samenwerkingsverbanden.....	13
3.3 Het beleid ten aanzien van het delen van cliëntgegevens	13
3.4 De praktijk ten aanzien van het delen van cliëntgegevens intern	14
3.5 De praktijk ten aanzien van het delen van gegevens met externen	15
3.6 Bevindingen van de onderzoeker.....	16
3.7 Ten slot.....	16
Hoofdstuk 4. College bescherming persoonsgegevens	17
4.1 Taken	17
4.2 Controle op het College Bescherming Persoonsgegevens.....	18
4.3 Sancties	18
4.4 De toegang tot het digitaal cliëntdossier	19
4.5 Delen van persoonsgegevens in samenwerkingsverband	20
4.6 Slot	22
Hoofdstuk 5. De juridische grenzen.....	23

5.1 Het internationaal juridische kader	23
5.1.1 <i>Inwerking treden van bepalingen uit internationale verdragen</i>	23
5.1.2 Gezondheidsrecht en recht op privacy in Internationale verdragen	24
5.2 Het nationaal juridisch kader	24
5.2.1 De Wet bescherming persoonsgegevens	24
5.2.1.1 Achtergrond	24
5.2.1.2 Reikwijdte van de Wbp	26
5.2.1.3 Plichten van de verantwoordelijke	28
5.2.1.4 Rechten van betrokkene	32
5.2.2 Geneeskundige behandelovereenkomst	33
5.2.2.1 Achtergrond	33
5.2.2.2 Reikwijdte WGB0	34
5.3 Algemene Verordening Gegevensbescherming	36
5.4 Slot	38
Hoofdstuk 6. Conclusies en aanbevelingen	39
6.1 Conclusies	39
6.1.1 De toegang tot digitale cliëntdossiers	39
6.1.1.1 Autorisatie van de toegang tot het digitaal cliëntdossier	39
6.1.1.2 Logging en controle	40
6.1.1.3 Beveiliging toegang	40
6.1.2 Delen van informatie	41
6.1.2.1 Delen van informatie intern	41
6.1.2.2 Delen van informatie extern	42
6.1.3 Algemene Verordening Gegevensverwerking	42
6.1.3 Wbp en WGB0	43
6.1.4 Slot	44
6.2 Aanbevelingen	44
6.2.1 toegang tot digitale cliëntdossiers	44
6.2.2 Beveiliging toegang	44
6.2.3 Delen van gegevens	44
6.2.4 Algemene Verordening Gegevensbescherming	45
6.2.4 Wbp en WGB0	45
Literatuurlijst	46
Bijlagen	47

Samenvatting

Traverse verwerkt gegevens in de zin van Wbp met als doel een optimale begeleiding van haar cliënten. De persoonsgegevens worden opgeslagen in het cliëntregistratiesysteem Regas Webbased en de toegang tot de digitale dossiers zijn beveiligd met een inlognaam en een wachtwoord. De autorisatie voor de toegang wordt verleend aan medewerkers op basis van hun functie. Er is door Traverse geen beleid gecodificeerd waarin is geregeld wie welke rechten krijgt ten aanzien van de digitale dossiers. Dit maakt het voor de medewerkers van de afdeling Automatisering moeilijk om verzoeken tot toegang tot dossiers te beoordelen.

Elke actie die plaatsvindt in het digitaal dossier wordt gelogd, dit is een wettelijk vereiste. De regelmatige controle op de logging is ook een vereiste uit de Wbp, maar dit wordt door Traverse nog niet toegepast. Op dit punt handelt Traverse in strijd met de Wbp die de verantwoordelijke verplicht passende technische en organisatorische maatregelen te implementeren om persoonsgegevens te beveiligen.

Om de cliënt optimaal te kunnen begeleiden deelt Traverse haar gegevens intern en met externen. Bij het delen van gegevens moet volgens het beleid van Traverse afgewogen worden of het doel van het delen van de gegevens het optimaal kunnen begeleiden van de cliënt is, of het delen van de gegevens nodig is om een overeenkomst uit te voeren waarbij de betrokkene partij is en wanneer gegevens met externen worden gedeeld of de cliënt hiervoor toestemming heeft gegeven. Deze afwegingen worden intern onvoldoende gemaakt. Uit interviews is gebleken dat de medewerkers zich niet bewust zijn van deze voorwaarde wanneer met collega's gegevens worden gedeeld. Daarnaast worden de gegevens onbewust gedeeld doordat ruimtes niet worden afgesloten. Het delen van persoonsgegevens gebeurt daardoor intern vaak onrechtmatig omdat Traverse zich niet houdt aan de Wet bescherming persoonsgegevens.¹

Er zijn, in tegenstelling tot het delen van informatie intern, meer medewerkers zich bewust van het geldende beleid bij het delen van gegevens met externen. Traverse deelt ook gegevens binnen samenwerkingsverbanden. De partijen binnen deze samenwerkingsverbanden zijn actief bezig met het opstellen van juridische kaders zodat effectiever gegevens gedeeld kunnen worden en er betere begeleiding voor de cliënt mogelijk is.

Naast de Wbp is in een aantal processen van Traverse ook de WGBO van toepassing en daarbij het beroepsgeheim. De WGBO is van toepassing op handelingen die onder de geneeskundige behandeling vallen, zoals het intramusculair toedienen van medicijnen, en alle handelingen die noodzakelijk samenhangen met deze behandeling. Op het verdere begeleidingsproces dat niet noodzakelijk is voor de geneeskundige behandeling van de cliënt is de Wbp van toepassing. De relevante handelingen van Traverse zijn het bepalen van bloedglucosewaarde, intramusculair injecteren, subcutaan injecteren, toedienen van insuline en het toedienen en verstrekken van medicatie.

In de nabije toekomst zal de inwerkingtreding van de Algemene Verordening Gegevensbescherming een aantal veranderingen met zich meebrengen ten opzichte van de huidige privacy wetgeving. Belangrijke veranderingen voor Traverse zijn onder andere dat

¹ Art. 8 Wbp.

een functionaris voor gegevensbescherming aangesteld moet worden, dat Traverse een transparant privacybeleid op moet stellen dat eenvoudig toegankelijk is, dat ze bij verwerkingen die bijzondere risico's inhouden een beoordeling moeten uitvoeren over het effect van de beoogde verwerkingen op de bescherming van persoonsgegevens en dat cliënten het recht krijgen om vergeten te worden.

Lijst van afkortingen

Art.	Artikel
BW	Burgerlijk Wetboek
CBP	College bescherming persoonsgegevens
ESH	Het Europees Sociaal Handvest
EVRM	Europees Verdrag voor de Rechten van de Mens
GW	Grondwet
IVBPR	Internationaal verdrag inzake Burger- en Politieke Rechten
IVESCR	Internationaal Verdrag inzake Economische, Sociale en Culturele Rechten
UVRM	Universele verklaring van de rechten van de mens
Wbp	Wet bescherming persoonsgegevens
WGBO	Wet op de geneeskundige behandelingsovereenkomst
Wob	Wet openbaarheid van bestuur

Begrippenlijst Wbp

- **Persoonsgegevens:** elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijk persoon.
- **Verwerking van persoonsgegevens:** elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.
- **Bestand:** elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen.
- **Verantwoordelijke:** de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt
- **Bewerker:** degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.
- **Betrokkene:** degene op wie een persoonsgegeven betrekking heeft
- **Derde:** ieder, niet zijnde de betrokkene, de verantwoordelijke, de bewerker, of enig persoon die onder rechtstreeks gezag van de verantwoordelijke of de bewerker gemachtigd is om persoonsgegevens te verwerken
- **Ontvanger:** degene aan wie de persoonsgegevens worden verstrekt
- **Toestemming van de betrokkene:** elke vrije, specifieke en op informatie berustende wilsuiting waarmee de betrokkene aanvaardt dat hem betreffende persoonsgegevens worden verwerkt
- **Verstrekken van persoonsgegevens:** het bekend maken of ter beschikking stellen van persoonsgegevens
- **Verzamelen van persoonsgegevens:** het verkrijgen van persoonsgegevens

Hoofdstuk 1. Inleiding

1. Inleiding

Dit hoofdstuk is het inleidende hoofdstuk van het onderzoeksrapport. In paragraaf 1 wordt de probleembeschrijving gegeven. In paragraaf 2 vindt men vervolgens de doelstelling en in paragraaf 3 de vraagstelling. In paragraaf 4 is aangegeven door middel van welke methodische aanpak onderzoek is gedaan om antwoord te kunnen geven op de vraagstelling. Als laatste wordt vervolgens in paragraaf 5 de opbouw van het onderzoeksrapport weergegeven.

1.1 Probleembeschrijving

In het kader van zorg en begeleiding verwerkt Traverse gegevens over haar cliënten. In het privacyreglement van Traverse is aangegeven op welke wijze met persoonsgegevens om dient te worden gegaan en welke rechten en plichten er voortvloeien uit de relevante wet- en regelgeving. Volgens dit reglement worden gegevens als naam, adres, woonplaats, geslacht, geboortedatum, telefoonnummer, nationaliteit, burgerlijke staat, gegevens over inkomsten/ uitgaven, zorggegevens, gegevens over medicatie en gegevens over voortgang gedurende de begeleiding verwerkt. Er wordt verder in het privacyreglement vermeld dat alle gegevens die van belang zijn voor de begeleiding (kunnen) worden verwerkt. Ook worden gegevens verwerkt die zijn aangeleverd door externe instanties.

In 2011 heeft er een reorganisatie plaatsgevonden binnen Traverse en is er dusdanig veel gewijzigd in de werkwijze dat men twijfelt of het beleid en de manier van werken nog voldoet aan de Wet bescherming persoonsgegevens (Wbp). Er is gekozen om voortaan procesgestuurd te werken. Zo maakt men sinds de reorganisatie gebruik van een zogenaamde Trajectregisseur. De Trajectregisseur is verantwoordelijk voor de cliënt en stuurt het proces vanaf de diagnose fase totdat de cliënt 'geholpen' is. De daadwerkelijke begeleiding wordt uitgevoerd door de toegewezen begeleiders van de inhoudelijke deskundigheidsgebieden: woonbegeleiding, dagbesteding, financiën en gezondheid. Op deze manier zijn er rondom de cliënt kleine teams georganiseerd, die zich van begin tot eind bekommeren om het, met de cliënt vooraf vastgestelde, eindresultaat. Deze manier van werken heeft tot gevolg dat veel medewerkers, die betrokken zijn bij de cliënt, via deze begeleiding, toegang hebben tot de digitale cliëntdossiers.

Een andere belangrijke wijziging is dat er sinds enkele weken gewerkt wordt met zogenaamde Toppers. Dit zijn werknemers die op verschillende afdelingen inzetbaar zijn. Dit betekent dat deze medewerkers met veel cliënten in aanraking zullen komen en dat er daarom goed nagedacht zal moeten worden op welke manier je deze werknemers toegang tot digitale cliëntdossiers geeft en wanneer.

Het college bescherming persoonsgegevens heeft deze zomer een rapport opgeleverd waaruit naar voren komt dat de onderzochte instellingen op het gebied van zorg niet voldeden aan de Wet bescherming persoonsgegevens waar het de toegang tot het digitale cliëntdossiers betrof.² Daarnaast zijn in de nabije toekomst wijzigingen in de regelgeving te verwachten door de toekomstige Europese regelgeving in de vorm van de Algemene Verordening Gegevensbescherming. Wanneer deze verordening in werking treedt heeft deze

² *Toegang tot digitale cliëntdossiers binnen zorginstellingen* (rapport van het CBP), Den Haag: juni 2013.

rechtstreekse werking in de lidstaten van de EU. Hierdoor zal de Wbp in de toekomst aangepast of vervangen worden.³

Daarnaast deelt Traverse cliëntgegevens met derden. Dit gebeurt zowel digitaal als in overlegsituaties. Traverse werkt samen met andere organisaties in het zorg- en veiligheidshuis en in het Housing First project. Binnen deze samenwerkingsverbanden worden ook persoonsgegevens gedeeld. Cliënten geven schriftelijk toestemming door in de begeleidingsovereenkomst te tekenen voor de gegevensuitwisseling met specifieke instanties ofwel door het ondertekenen van een apart toestemmingsformulier uit Regas. Regas is een internationaal cliëntregistratiesysteem en wordt in Nederland, België en Duitsland aangeboden. Of Traverse hiermee voldoet aan de wettelijke verplichtingen en de privacy van cliënten voldoende beschermt is voor Traverse niet duidelijk.

Wanneer Traverse handelt in strijd met de wet zouden er sancties opgelegd kunnen worden en dit maakt het noodzakelijk dat Traverse een beleid heeft dat overeenstemt met de wet en regelgeving en dat het beleid ook wordt nageleefd. Nog belangrijker dan sancties die opgelegd kunnen worden is dat de privacy van cliënten van Traverse voldoende moet zijn beschermd, dit is mogelijk niet het geval als Traverse handelt in strijd met de wet.

De toekomstige Europese wijziging zoals deze eerder beschreven is zal in alle waarschijnlijkheid in een korte periode na dit onderzoek in werking treden. Dit maakt dat het noodzakelijk is om de verordening te betrekken bij het onderzoek om geen verouderde informatie te leveren.

Het bovenstaande is voor Traverse aanleiding voor een onderzoek naar de toegang tot de digitale cliëntgegevens en de informatie-uitwisseling binnen Traverse en vanuit Traverse naar externen.

1.2 Doelstelling

Op 7 januari een onderzoeksrapport opleveren aan Traverse. Door de huidige werkwijze van Traverse aan de Wet bescherming persoonsgegevens en de toekomstige Europese wijziging op het gebied van privacy recht te toetsen worden conclusies getrokken over de rechtmatigheid van de huidige werkwijze en worden aanbevelingen gedaan waardoor de opdrachtgever eventuele onrechtmatige situaties kan voorkomen.

1.3 Vraagstelling

Centrale vraag:

Welke aanbevelingen kunnen er worden gedaan over de bescherming van de privacy van cliënten van Traverse, met betrekking tot de toegang tot digitale cliëntdossiers en het delen van persoonsgegevens intern en in samenwerking/contact met derden, gelet op de wettelijke verplichtingen?

1.4 Onderzoeksmethodiek

De gekozen onderzoeksstrategieën zijn een onderzoek van het recht en een onderzoek van de praktijk geweest. Voor het onderzoek naar het recht zijn rechtsbronnen en literatuur geanalyseerd en onderling vergeleken. De Verordening Bescherming Persoonsgegevens is

³ www.eerstekamer.nl → zoek: E120003.

vergeleken met bestaande wetgeving en de Wbp is vergeleken met de WGBO, geanalyseerd en geïnterpreteerd met gebruik van de memorie van toelichting van de Wbp.

Voor het onderzoek naar de praktijk is kwalitatief onderzoek verricht. Er is gebruik gemaakt van semigestructureerde interviews met medewerkers van Financiën, Automatisering en Regie. De keuze voor deze medewerkers is gemaakt nadat werd vastgesteld dat deze medewerkers vaak met persoonsgegevens werken en in overleg situaties persoonsgegevens delen. Er is gekozen voor semigestructureerde interviews om specifieke informatie te kunnen vergelijken, terwijl ruimte werd gelaten voor extra informatie vanuit de geïnterviewde. Daarnaast zijn er semigestructureerde interviews gehouden met teamleiders om te toetsen of ze op de hoogte waren van omgang met persoonsgegevens van de medewerkers. Ook bood deze interviewmethode meer ruimte aan de teamleiders om vanuit zichzelf informatie te verschaffen over de wijze waarop informatie wordt ingezien en verwerkt in overlegsituaties met externen.

1.5 Opbouw van het rapport

Het onderzoeksrapport is als volgt opgebouwd. In hoofdstuk 2 wordt aandacht besteed aan de toegang tot het digitaal cliëntdossier. Hier wordt uitgelegd wat het beleid van Traverse met betrekking tot deze toegang is en wordt beschreven hoe daar in de praktijk mee om wordt gegaan. In hoofdstuk 3 wordt het delen van persoonsgegevens beschreven. Het gaat daarbij om zowel interne gegevensuitwisseling als externe. Eerst wordt, net als in hoofdstuk 2, het beleid ten aanzien van het delen van gegevens toegelicht om vervolgens de praktijk met betrekking tot het delen van de gegevens toe te lichten. Er is in de beschrijving van de praktijk een onderscheid gemaakt in het delen van gegevens intern en met externen. In hoofdstuk 4 wordt het College Bescherming Persoonsgegevens (CBP) nader toegelicht met betrekking tot hun taken. Ook wordt de controle op het CBP toegelicht. Verder wordt ingegaan op de sanctiebevoegdheid van het CBP. Ten slotte is in dit hoofdstuk beschreven wat het CBP zegt over de toegang tot digitale cliëntdossiers en het delen van persoonsgegevens in samenwerkingsverband. In hoofdstuk vijf wordt vervolgens het wettelijk kader geschetst met betrekking tot de bescherming van persoonsgegevens. Daarbij komt zowel internationale als nationale wetgeving aan bod en wordt ook de Algemene Verordening Gegevensbescherming besproken. Het rapport wordt afgesloten met hoofdstuk 6 waarin de conclusies en aanbevelingen zijn opgenomen.

Hoofdstuk 2. Toegang digitaal cliëntdossier

In dit hoofdstuk zal worden ingegaan op de huidige werkwijze van Traverse met betrekking tot de toegang tot digitale cliëntdossiers. Er zal worden beschreven wat het beleid van Traverse nu is en of dit beleid in de praktijk wordt nageleefd. In paragraaf 1 wordt toegelicht wat er voorafgaat aan de aanleg van het dossier en welke informatie in het dossier opgeslagen wordt. In paragraaf 2 wordt het beleid dat geldt uitgelegd, in paragraaf 3 wordt de praktijk uitgewerkt en in paragraaf 4 volgt het slot met daarin een conclusie.

2.1 Het digitaal cliëntdossier

Wanneer een persoon zich meldt bij Traverse zal een medewerker van aanmelding en intake toetsen of diegene in aanmerking komt voor begeleiding en / of behandeling. De belangrijkste vragen die gesteld worden bij de intake hebben betrekking op de vraag of iemand dak- of thuisloos is geraakt of dreigt te raken, of er sprake is van Multi-problematiek en of de cliënt al historie binnen Traverse heeft opgebouwd. Als tijdens de intake de eerste twee vragen een positief antwoord opleveren en de cliënthistorie geen beperkingen omvat, wordt de cliënt toegelaten. Binnen 48 uur zal definitief tot aanname besloten moeten zijn en wordt de cliënt overgedragen aan een Trajectregisseur. De Trajectregisseur zal de indicatiestelling op zich nemen. Om tot een indicatiestelling te komen zal de Trajectregisseur diverse informatiebronnen moeten raadplegen zoals; collega's, te raadplegen cliënthistorie, huisartsen, psychiaters, familie, school, maatschappelijk werk etc. Op deze manier wordt er een cliëntdossier met daarin een indicatiestelling met betrekking tot de problematiek van de cliënt samengesteld.

Het cliëntdossier bestaat uit twee delen, namelijk een papieren dossier en een digitaal dossier in Regas. In de papieren dossiers zijn vooral ondertekende papieren opgenomen. Het vult daarmee het digitale dossier, die de meeste informatie bevat, aan. De manier waarop het dossier samengesteld moet worden is opgenomen in een intern document 'de werkinstructie cliëntdossier'.⁴ De werkinstructie cliëntdossier is vooral gericht op het papieren dossier. Wel is er een checklist opgenomen die een opsomming geeft welke documenten minimaal opgenomen moeten zijn voor zowel het papieren als het digitale dossier. In de checklist is te zien welke medewerkers van Traverse verantwoordelijk zijn voor bepaalde informatie, en welke medewerkers daarmee dus betrokken zijn en inzage hebben in het digitaal cliëntdossier. Genoemd worden de Intaker, Trajectregisseur, Indicatiefunctionaris, Woonbegeleider, Verzorgende/Verpleegkundige en Financieel begeleider. Deze checklist is opgenomen in de bijlage.

2.2 Het beleid met betrekking tot de toegang tot digitale cliëntdossiers

Zoals in de vorige paragraaf is beschreven bevat het digitale cliëntdossier persoonsgegevens van de cliënt. Het beleid van Traverse met betrekking tot privacy is vastgelegd in het protocol bescherming persoonsgegevens cliënten en is voor alle medewerkers te raadplegen via het digitale kwaliteitshandboek. In dit protocol wordt een overzicht van de vereisten uit de Wbp gegeven en de wijze waarop Traverse hier in de praktijk vorm aan heeft gegeven.

⁴ Zie bijlage 5.

Het beleid rondom de toegang tot digitale cliëntgegevens is nergens schriftelijk vastgelegd op de werkinstructie cliëntdossier na. De werkinstructie laat echter alleen zien wie verantwoordelijk is voor het plaatsen van de informatie in het dossier. Hoewel daar uit kan worden opgemaakt wie er toegang heeft staat dit nergens specifiek beschreven. Voor de reorganisatie was er wel gecodificeerd beleid met betrekking tot wie wanneer toegang kreeg tot een cliëntdossier, maar het is nu nergens meer terug te vinden. De reden hiervoor zou kunnen zijn dat Traverse vanaf de reorganisatie werkt met het digitale handboek waar alle processen, werkbeschrijvingen en belangrijke documenten worden opgeslagen en deze hier te raadplegen zijn. Voor de reorganisatie bestond dit handboek nog niet en waarschijnlijk is het beleid rondom de toegang tot digitale cliëntdossiers niet overgezet naar het huidige handboek.

2.3 De praktijk met betrekking tot de toegang tot digitale cliëntdossiers

2.3.1 De toegang

Tijdens de onderzoeksperiode is Traverse overgestapt van het oude digitale cliëntregistratiesysteem Regas naar het huidige digitale cliëntregistratiesysteem Regas Webbased. In deze paragraaf zal eerst de oude situatie worden besproken waarna vervolgens de huidige situatie aan de orde komt.

Iedere medewerker had tijdens de oude situatie een username en wachtwoord om in te loggen in Regas. Vanwege licentietekorten is er toentertijd voor gekozen om alle medewerkers van de afdeling beleid dezelfde username en hetzelfde wachtwoord te geven voor Regas. Dit is ook gedaan voor de receptie. De medewerkers van beleid en de receptie konden volgens de afdeling automatisering alleen gegevens inzien en niets invoeren of wijzigen in het cliëntsysteem. Een enkele werknemer gaf echter aan wel informatie te kunnen invoeren of wijzigen. Traverse is er bij deze werkwijze van uit gegaan dat de digitale cliëntdossiers voldoende beveiligd waren. Hierbij is men er, onterecht, van uit gegaan dat er niks in de gegevens gedaan kon worden en dat medewerkers een verklaring tekenen wanneer ze in dienst treden waarin is opgenomen dat er vertrouwelijk met de gegevens dient te worden omgegaan. Deze verklaringen hebben echter nooit bestaan binnen Traverse en zijn dus ook nooit ondertekend.

Sinds de invoering van Regas Webbased wordt er autorisatie voor toegang tot digitale cliëntdossiers verleend op grond van de functie die een medewerker heeft. Daarbij wordt een onderscheid gemaakt tussen medewerkers die betrokken zijn bij het beheer van de instelling en medewerkers die zijn betrokken bij de behandeling of begeleiding van cliënten. De afdeling automatisering krijgt door van personeelszaken wie er in dienst treedt en of er mutaties zijn wanneer iemand van functie wisselt. Aan de functie is de toegang die de medewerkers van automatisering verlenen tot Regas gekoppeld (Regas is het cliëntregistratiesysteem dat Traverse gebruikt). Er wordt onderscheidt gemaakt in bepaalde functies op basis van werkcontext. De trajectregisseurs krijgen toegang tot de gegevens van alle cliënten in Regas en de woonbegeleiders kunnen bij alle collega woonbegeleiders de cliëntendossiers zien. Er wordt bij de woonbegeleiders wel onderscheidt gemaakt in zelfstandig woonbegeleider en onzelfstandig woonbegeleider. Dat wil zeggen dat de zelfstandig woonbegeleiders alleen in de cliëntdossiers van andere zelfstandig woonbegeleiders kunnen en ditzelfde geldt voor de onzelfstandig woonbegeleiders.

Toegang tot dossiers waartoe de medewerker op basis van zijn of haar functie geen toegang heeft wordt door de medewerkers van de afdeling automatisering op gewoonte en onderbuikgevoel verleend. Men gaf aan dat wanneer er speciale verzoeken binnen kwamen om cliëntdossiers in te kunnen zien wanneer hier nog geen autorisatie voor verleend was, ze de toegang toekenden of afkeurden op onderbuikgevoel. Daarbij wegen zij zelf af of naar hun mening hiermee de privacy van de cliënt in het gedrang zou kunnen komen. De medewerkers van de afdeling automatisering gaven aan dat zij het lastig vinden dat niet is vastgelegd wie wanneer en waarvoor geautoriseerd mag worden.

Ook nieuw binnen Traverse zijn de zogenaamde Toppers. Dit zijn medewerkers die Multi-inzetbaar zijn. Deze medewerkers moeten op alle functies van Traverse kunnen worden ingezet en zij zullen ook regelmatig wisselen van functie. Deze Toppers hebben alle rechten voor Regas Webbased gekregen die ze, in de functies die ze zouden kunnen vervullen, nodig zouden hebben. Afgesproken is dat deze rechten onmiddellijk komen te vervallen zodra de medewerker uit de functie van Topper is.

Ook zal vanaf 1 januari 2014 van elke nieuwe medewerker en vrijwilliger worden verwacht dat ze een verklaring omtrent gedrag afgeven. Wat betreft de huidige werknemers zal enkel aan de werknemers van de afdeling financiën worden gevraagd om een verklaring omtrent gedrag af te geven.

2.3.2 Logging

Wanneer mensen inlogden in Regas werd dit geregistreerd en kon er worden terug gevonden in welke dossiers iemand iets heeft gewijzigd. Dit heet logging. Uit de wet vloeit voort dat zorginstellingen structureel moeten bijhouden wie wanneer welk patiëntendossier heeft geraadpleegd (logging) en dat dit wordt gecontroleerd. Mevrouw van der Beemt, medewerker automatisering van Traverse, gaf aan dat er bij Traverse alleen controle plaatsvond op basis van klachten of wanneer er iets ongewoons opgemerkt werd. Dit betekent dat er nooit controle plaatsvond wanneer mensen slechts persoonsgegevens inzagen en niks wijzigden, er is dan immers geen opmerkelijkheid die de aandacht trekt.

Sinds de invoering van Regas Webbased wordt ook geregistreerd wanneer men inlogt om alleen dossiers in te zien en wordt dit allemaal gelogd. Daarnaast heeft iedereen in deze nieuwe versie een eigen username en wachtwoord, dus ook de afdeling beleid en de receptie. Er is echter nog geen systematische controle op de gelogde gegevens.

2.4 Ten slot

Traverse heeft met betrekking tot de toegang tot het digitale cliëntdossier nauwelijks geschreven beleid. Er is wel beleid waarin opgenomen is welke afdelingen welke autorisatie krijgen, dit is alleen niet gecodificeerd. Dit geldt echter nog niet voor de sinds kort ontstane functie 'de Toppers'. Deze medewerkers zijn overal inzetbaar en er is voor gekozen hen alle mogelijke rechten van de functies die ze zouden kunnen vervullen, te geven.

Sinds Traverse is overgestapt van Regas op Regas Webbased heeft iedere medewerker zijn eigen inlognaam en wachtwoord voor Regas, wat in het verleden niet het geval was. Toentertijd had de gehele afdeling beleid en de receptie hetzelfde wachtwoord en dezelfde inlognaam. Hierdoor was een specifieke logging en controle hierop onmogelijk. Er is net als voorheen, toen nog gewerkt werd in Regas, geen systematische controle op de logging.

Hoofdstuk 3. Het delen van cliëntgegevens

In dit hoofdstuk wordt toegelicht welke cliëntgegevens gedeeld worden, door wie dit gebeurt en met wie de gegevens gedeeld worden. Voor dit uitgewerkt wordt, wordt het beleid van Traverse ten aanzien van het delen van gegevens zowel onderling als met derden toegelicht. In paragraaf 1 worden kort de contacten van Traverse beschreven en in paragraaf 2 de samenwerkingsverbanden. In paragraaf 3 wordt ingegaan op het beleid van Traverse ten aanzien van het delen van persoonsgegevens. Paragraaf 4 beschrijft de praktijksituatie met betrekking tot het delen van gegevens intern en paragraaf 5 beschrijft de praktijksituatie met betrekking tot het delen van persoonsgegevens met externen. In paragraaf 6 worden de bevindingen van de onderzoeker beschreven en in paragraaf 7 volgt het slot met de conclusie.

3.1 Contacten

De cliënten van Traverse hebben te maken met problemen op verschillende levensterreinen. Traverse werkt daarom nauw samen met onder andere geestelijke gezondheidszorg, verslavingszorg, reclassering, ouderenzorg, sociale dienst, jeugdzorg, woningcorporaties en politie. In dit onderzoek is gekeken naar twee samenwerkingsverbanden waarbinnen Traverse cliëntgegevens deelt. Dit zijn het Zorg- en Veiligheidshuis Midden- Brabant en Housing First Tilburg.

3.2 De samenwerkingsverbanden

“Het Zorg- en Veiligheidshuis Midden-Brabant is een samenwerkingsverband van 20 partnerorganisaties die werken aan een gezamenlijke aanpak van sociale veiligheid. Het Veiligheidshuis is in 2002 opgericht door de gemeente Tilburg, Politie Midden- en West Brabant en het Openbaar Ministerie Breda. In 2008 is het Zorghuis opgericht. Het Zorghuis richt zich op volwassenen en gezinnen met een meervoudige en complexe problematiek. Zorgpartners maken onder regie van de gemeente één integraal en bindend plan van aanpak voor deze mensen.”⁵

Housing First Tilburg is een samenwerkingsverband tussen GGZ-Breburg, Novadic-Kentron, RIBW Brabant, Traverse, VOF Dubbele Diagnose en de Tilburgse woningcorporaties. Het doel van Housing First Tilburg is om binnen 2 jaar tijd tachtig daklozen aan een woning te helpen. Het gaat om personen voor wie de bestaande route van zorg en opvang naar begeleid wonen geen optie is. Dit heeft te maken met het niet passen in woongroepen door hun gedrag. Door deze personen meteen een eigen woning te bieden krijgen ze de rust om een toekomst op te bouwen. Ze krijgen daarbij hulp met het beteugelen van verslaving of bij financiën.⁶

3.3 Het beleid ten aanzien van het delen van cliëntgegevens

In het kader van zorg en begeleiding verwerkt Traverse gegevens over haar cliënten. In het privacyreglement van Traverse is aangegeven op welke wijze met persoonsgegevens om dient te worden gegaan en welke rechten en plichten er voortvloeien uit de wet. Volgens dit reglement worden gegevens als naam, adres, woonplaats, geslacht, geboortedatum, telefoonnummer, nationaliteit, burgerlijke staat, gegevens over inkomsten/ uitgaven,

⁵ www.tilburg.veiligheidshuis.org.

⁶ www.smo-traverse.nl → zoek: Housing First → ondertekening Housing First Tilburg.

zorggegevens, gegevens over medicatie, en gegevens over de voortgang gedurende de begeleiding verwerkt. Er wordt verder nog vermeld dat alle gegevens die van belang zijn voor de begeleiding (kunnen) worden verwerkt. Ook worden gegevens verwerkt die zijn aangeleverd door externe instanties.

Traverse heeft geen specifiek beleid ten aanzien van het delen van persoonsgegevens. Ze hebben wel een protocol bescherming persoonsgegevens cliënten waarin gesproken wordt over het verwerken van persoonsgegevens. In het protocol is opgenomen dat het doel van de verwerking van persoonsgegevens het optimaal kunnen begeleiden van cliënten is. Het delen van persoonsgegevens valt onder het begrip verwerken in de zin van de Wbp. Wanneer gegevens gedeeld worden door Traverse moet volgens het eigen beleid dus altijd afgewogen worden of het delen van de gegevens noodzakelijk is voor het optimaal kunnen begeleiden van de cliënt.

De grondslag voor de verwerking van gegevens is volgens het protocol art.8 sub b Wbp. Dit betekent dat het verwerken en daarmee het delen van gegevens rechtmatig is wanneer de verwerking plaats vindt om een overeenkomst uit te voeren waarbij de betrokkene partij is.

Verder wordt er in het protocol beschreven dat de cliënt voor het delen van gegevens met externen toestemming geeft, en dat deze toestemming schriftelijk geschiedt. In de werkinstructie Aanmelding en Intake is een bijlage opgenomen: checklist bij Intake. In deze checklist staat dat akkoord moet zijn gegaan met gegevensuitwisseling met derden. Dit akkoord is in de vorm van een toestemmingsformulier dat moet worden ondertekend door de cliënt bij intake. Dit document wordt bewaard in Regas en in het papieren cliëntdossier. Medewerkers kunnen op deze manier zien of de cliënt getekend heeft voor het delen van de gegevens met externen. Het toestemmingsformulier geldt voor het gehele begeleidingstraject van de cliënt.

3.4 De praktijk ten aanzien van het delen van cliëntgegevens intern

Intern wordt veel samengewerkt. Zo heeft de afdeling Regie contact met alle interne partijen omdat zij de rode draad is in de begeleiding van de cliënt. De afdeling financiën heeft ook veel contact met woonbegeleiders. Door middel van interviews is duidelijk geworden dat het beleid zoals in de vorige paragraaf omschreven niet goed bekend is bij de medewerkers. Men gaf aan zich bewust te zijn van het beleid maar kon dit beleid vervolgens niet toelichten. De enige voorwaarden waar iedereen zich bewust van is, is de toestemming die nodig is voor het delen van de gegevens met externen. Intern worden gegevens bewust en onbewust gedeeld. Bewust worden gegevens van cliënten gedeeld in overlegsituaties en digitaal via mailwisseling. Wanneer in overlegsituaties gegevens van een cliënt gedeeld worden, wordt door de medewerkers nauwelijks afgewogen of deze informatie noodzakelijk is om het doel te dienen waarvoor de gegevens oorspronkelijk verzameld zijn. Dit blijkt uit gesprekken met teamleiders, medewerkers en uit de eigen bevindingen van de onderzoeker. Doordat deze afweging niet plaatsvindt wordt er meer informatie gedeeld dan nodig is voor de uitvoering van de taak van de medewerker.

Hoewel de medewerkers die betrokken zijn bij de cliënt toegang hebben tot het digitaal cliëntdossier in Regas Webbased worden er ook gegevens gedeeld via mailwisseling. Dit blijkt uit gesprekken met medewerkers en de teamleider van Financiën en Regie.

De teamleider van de afdeling Financiën en Regie geeft daarnaast aan dat door het ontbreken van duidelijk beleid over het delen van gegevens van cliënten ze haar eigen referentiekader gebruikt. Ze probeert zoveel mogelijk te vermijden overbodige informatie te verstrekken en te spreken over 'cliënt' en hierbij geen namen te noemen als dit niet

noodzakelijk is. Ze benoemt daarnaast dat het opmerkelijk is hoe vrijelijk er over cliënten wordt gesproken binnen Traverse.

Naast het bewust delen van gegevens worden ook onbewust gegevens gedeeld. Het onbewust delen van gegevens gebeurt onder andere op momenten dat cliënten telefonisch contact opnemen met de receptie. Tijdens deze gesprekken noemt de receptioniste vaak hardop de naam en problematiek van de cliënt over wie het telefoongesprek gaat. De deur tussen de receptieruimte en een kantoorruimte staat regelmatig open. Hierdoor zijn de gesprekken hoorbaar in de gang en op diverse werkplekken. Dit zelfde geldt voor wanneer een cliënt aan de balie staat bij de receptionist.

Verder worden er vaak casussen besproken waarbij deuren worden opengelaten en informatie over cliënten hoorbaar is in andere ruimtes of wordt dit besproken in een kantoorruimte met meerdere medewerkers die niet betrokken zijn bij de cliënt.

3.5 De praktijk ten aanzien van het delen van gegevens met externen

Uit interviews is naar voren gekomen dat men, vergeleken met het intern delen van informatie, beter op de hoogte is van wanneer medewerkers persoonsgegevens van cliënten mogen delen met externen. Traverse deelt persoonsgegevens van cliënten met externen wanneer dit van belang is voor de behandeling/ begeleiding van de cliënt. Dit kan zijn met de huisarts, GGZ, woningcorporaties, zorgverzekeraars, belastingdienst etc. Voor de uitwisseling van deze gegevens wordt toestemming gevraagd aan de cliënt door middel van het toestemmingsformulier dat in de vorige paragraaf is genoemd. Een aantal medewerkers gaven aan alsnog contact op te nemen, om de cliënt te informeren zodra er overleg plaats zou vinden met bijvoorbeeld de huisarts. Een aantal medewerkers is op de hoogte dat alleen de gegevens die nodig zijn voor een goede begeleiding van de cliënt gedeeld mogen worden.

Traverse deelt naast met individuele externen, ook informatie binnen samenwerkingsverbanden. De samenwerkingsverbanden waar in dit onderzoek naar gekeken is, zijn het zorg- en veiligheidshuis en Housing First Tilburg.

Het zorg-en veiligheidshuis

Er is binnen het zorg-en veiligheidshuis al veel aandacht besteed aan het delen van informatie tussen verschillende partijen. Er is de zogenaamde 'leertuin' opgezet. 'Het doel van de leertuin Zorg-en veiligheid is te komen tot een eenduidige interpretatie van de wet- en regelgeving en een ontschot informatie uitwisseling'.⁷ De aanleiding voor dit project is een aantal terugkerende problemen, zoals het bespreken van personen waarbij onvoldoende gebruik werd gemaakt van beschikbare informatie, ketenpartners die ieder een eigen invulling gegeven aan welke informatie wanneer gedeeld mag worden en er zou doorgaans geen juridische afdekking zijn van de informatie die in een digitaal casus ondersteuningssysteem wordt vastgelegd. Door een generiek juridisch kader vast te stellen, kunnen professionals gegevens over hun cliënten delen. Hierdoor zou beter op elkaar afgestemde zorg mogelijk zijn. De brochure 'samenwerken in de jeugdketen, een instrument voor gegevensuitwisseling' uitgebracht door het ministerie VWS, wordt verder ontwikkeld in

⁷ www.tilburg-veiligheidshuis.org → Leertuin Zorg en Veiligheid → Nieuwsbrief Leertuin Zorg en Veiligheid mrt. 2013.

de Leertuin Zorg en Veiligheid zodat het op alle domeinen toepasbaar wordt.⁸ Er wordt in deze situaties met name ook gekeken naar de situaties waarneer de cliënt geen toestemming geeft voor het delen van de informatie maar de hulpverleners/professionals vinden het noodzakelijk voor de juiste begeleiding van de cliënt of om derden te beschermen dat deze informatie gedeeld wordt.

Housing First Tilburg

Ook binnen Housing First Tilburg (HFT) worden gegevens gedeeld ten behoeve van de begeleiding van de cliënt. Binnen HFT wordt uitgegaan van het beleid dat de organisatie zelf heeft. Er wordt gebruikgemaakt van het cliëntregistratiesysteem Regas Webbased. Op het snijvlak van het delen van informatie gebeurt het dat een partij van het samenwerkingsverband aangeeft dat bepaalde informatie niet wordt verstrekt. Er wordt voor deze gevallen gekeken naar de afspraken die zijn gemaakt bij het zorg-en veiligheidshuis. Verder is er een code voor informatiedeling afgesproken rondom bemoeizorg. Dit heeft betrekking op informatiedeling waar de cliënt geen toestemming voor geeft. Deze code wordt ook gebruikt.

Beide samenwerkingsverbanden zijn momenteel nog bezig een vaste werkwijze vast te stellen met betrekking tot het delen van informatie. Alvorens hierover definitieve afspraken worden gemaakt zou het kunnen lonen om hier juridisch kritisch naar te kijken.

3.6 Bevindingen van de onderzoeker

Tijdens mijn onderzoeksperiode van 3 maanden binnen de organisatie is het mij opgevallen hoe gemakkelijk er over cliënten wordt gesproken. Dit merkte ik op wanneer ik in bepaalde casussen ondersteuning bood, maar vooral in de tijdens het lopen door de Traverse gebouw. Er wordt nauwelijks gesproken over 'een cliënt' maar degene wordt meestal met naam en toenaam genoemd. Bij de receptie worden namen van cliënten genoemd in bijvoorbeeld telefoongesprekken of wanneer iemand aan de balie staat. Naast naam wordt ook geregeld een problematiek besproken zodat de receptioniste weet met wie ze diegene door moet verbinden of wat voor advies ze diegene moet geven. Hierdoor wordt geregeld een naam en casus hoorbaar voor andere medewerkers. Deze deling van persoonsgegevens is een deling die onbedoeld plaatsvindt. Deze constatering wordt ondersteunt door de teamleider Regie en Financiën. Er wordt binnen Traverse onvoldoende afgewogen of er sprake is van een noodzaak om bepaalde informatie te verstrekken.

3.7 Ten slot

Bij het delen van gegevens moet volgens het beleid van Traverse afgewogen worden of het doel van het delen van de gegevens het optimaal kunnen begeleiden van de cliënt is, of het delen van de gegevens nodig is om een overeenkomst uit te voeren waarbij de betrokkene partij is en wanneer gegevens met externen worden gedeeld of de cliënt hiervoor toestemming heeft gegeven. Het delen van gegevens binnen Traverse gaat gemakkelijk en er wordt weinig rekening gehouden met het beschermen van de privacy van de gegevens. Bij het delen van informatie met externen is het beleid beter bekend bij medewerkers. In samenwerkingsverband is men actief bezig met het verbeteren van efficiënte informatiedeling.

⁸ www.tilburg-veiligheidshuis.org → Leertuin Zorg en Veiligheid → Factsheet Leertuin Zorg en Veiligheid.

Hoofdstuk 4. College bescherming persoonsgegevens

In dit hoofdstuk wordt ingegaan op het College bescherming persoonsgegevens. In de paragraaf 1 worden de taken van het College beschreven, in paragraaf 2 de controle op het College en in paragraaf 3 de sancties die het College op kan leggen. Verder wordt in paragraaf 4 beschreven wat het College zegt over de toegang tot digitale cliëntdossiers en in paragraaf 5 wat het College opmerkt over het delen van persoonsgegevens in samenwerkingsverbanden. Vervolgens sluit paragraaf 6 het hoofdstuk af met een conclusie.

4.1 Taken

Het College bescherming persoonsgegevens (CBP) is op grond van Richtlijn 95/46/EG de toezichthoudende autoriteit die toezicht houdt op de naleving van wetten die het omgaan met persoonsgegevens regelen.⁹ In het bijzonder gaat het dan om de volgende wetten: Wet bescherming persoonsgegevens, de Wet politiegegevens en de Wet gemeenschappelijke basisadministratie persoonsgegevens. Het CBP bevordert het aanstellen van een functionaris voor de gegevensbescherming en stimuleert bedrijven een gedragscode op te stellen voor hun branche of sector.¹⁰

Het CBP heeft verschillende taken ter uitvoering van de Richtlijn 95/46/EG. Ze houden toezicht, adviseren, geven voorlichting, verstrekken informatie en hebben internationale taken. De taken worden hierna kort toegelicht.

Toezicht

Het CBP houdt toezicht op de naleving van wetten en toepassing van wetten die het omgaan met persoonsgegevens regelen. Toezicht houden op deze naleving houdt in dat ze onderzoek kunnen doen uit eigen beweging naar overtreding van de wet, zoals bijvoorbeeld onlangs bij een aantal apotheken gebeurd is.¹¹ Ze kunnen bestuursdwang toepassen of een bestuurlijke boete opleggen wanneer geconstateerd wordt dat de meldplicht wordt overtreden. Ze kunnen verder vooraf onderzoek doen naar de verwerking van persoonsgegevens die worden gemeld bij het CBP en waaraan bijzondere risico's zijn verbonden. Onder toezicht vallen ook nog activiteiten als het toetsen van gedragscodes, klachten behandelen over naleving van de Wbp en bemiddelen bij geschillen over de uitoefening van het recht op inzage, correctie of verzet. Verder houden ze een register bij van Wbp-meldingen, leggen ze een boete op bij overtreding van de meldingsplicht en verlenen ze ontheffingen op het verbod op verwerking van bijzondere persoonsgegevens.¹²

Advisering

Adviseren houdt in dat ze op grond van de Wbp of uit eigen beweging de regering en/of het parlement adviseren over voorgenomen wet- en regelgeving die betrekking heeft op de verwerking van persoonsgegevens. Daarnaast adviseren ze de minister van Justitie over doorgifte van persoonsgegevens naar derde landen. Derde landen, zijn landen buiten de Europese Unie.¹³

Voorlichting, informatieverstrekking en verantwoording

Met betrekking tot de uitleg van wettelijke normen proberen ze helderheid te verschaffen aan verantwoordelijken door middel van richtsnoeren of zienswijzen. Verder verstrekken ze veel

⁹ Richtlijn 95/46/EG (*PbEG* 1995, L281/31), art. 28.

¹⁰ www.CBPweb.nl → wetten en zelfregulering.

¹¹ www.CBPweb.nl → nieuws en publicaties → Apothekers treffen privacybeschermende maatregelen na onderzoeken CBP.

¹² www.CBPweb.nl → over het CBP.

¹³ www.CBPweb.nl → over het CBP.

informatie via de websites van het CBP en via het telefonisch spreekuur. Ten slotte publiceren ze jaarverslagen.¹⁴

Internationale taken

Het CBP is aangewezen als bevoegde autoriteit in de zin van het Verdrag van Straatsburg. Dit is het Dataprotectieverdrag van de Raad van Europa uit 1981. Artikel 18 van dit verdrag roept een adviescommissie in het leven. Voor Nederland is dit dus het CBP.¹⁵ Het CBP neemt daarnaast deel aan verschillende Internationale en Europese colleges, waaronder de werkgroep van Europese privacytoezichthouders, waarvan het CBP momenteel de voorzitter is. Verder vertegenwoordigen ze zich in verschillende toezichthoudende organen in EU-verband.¹⁶

4.2 Controle op het College Bescherming Persoonsgegevens

De controle op het CBP komt voornamelijk vanuit de burger. Op grond van artikel 56 lid 3 van de Wbp heeft het CBP een bestuursreglement vastgesteld waarin regels over de werkwijzen en procedures met het oog op een goede en zorgvuldige uitoefening van hun taken zijn gecodificeerd.¹⁷ Verder dan dit reiken de interne waarborgen echter niet. Het CBP is bij de uitvoering van zijn bevoegdheden gehouden aan de bepalingen van de Algemene wet bestuursrecht (Awb). Daarnaast is de Wet openbaarheid van bestuur (Wob) van toepassing en is het CBP als bestuursorgaan gebonden aan de algemene beginselen van behoorlijk bestuur.

De Wob regelt onder andere dat het bestuursorgaan informatie verstrekt overeenkomstig deze wet en dat het bestuursorgaan er zo veel mogelijk zorg voor draagt dat de informatie die overeenkomstig de wet wordt verstrekt actueel, nauwkeurig en vergelijkbaar is. Een ander belangrijk punt dat de Wob regelt is het verzoek om informatie dat is neergelegd in documenten over een bestuurlijke aangelegenheid die een ieder kan verzoeken.

De algemene beginselen van behoorlijk bestuur zijn beginselen die voortgekomen zijn uit jurisprudentie. Deze beginselen geven gedragsregels aan overheidsorganen met als doel de burger te beschermen tegen deze organen. De beginselen bestaan uit formele en materiële beginselen en aantal zijn opgenomen in de Awb.

Vanuit de burger is er ook veel mogelijk. Tegen besluiten van het CBP kan bezwaar worden gemaakt en beroep worden aangetekend bij de bestuursrechter en er kan een klacht worden ingediend bij de Nationale ombudsman.

4.3 Sancties

De Wbp geeft het CBP de bevoegdheid tot het toepassen van bestuursdwang ter handhaving van de verplichtingen die gesteld zijn door de Wbp. Wanneer naar het oordeel van het CBP wordt gehandeld in strijd met de Wbp, kan deze bevoegdheid worden uitgeoefend. De bestuursdwang vindt zijn grondslag in de Awb.¹⁸ Het valt onder het hoofdstuk herstelsancties omdat bestuursdwang erop gericht is een onrechtmatige situatie te herstellen. Ook de verplichtingen die gesteld worden aan een last onder bestuursdwang zijn

¹⁴ www.CBPweb.nl → over het CBP.

¹⁵ www.CBPweb.nl → over het CBP → CBP Internationaal → Raad van Europa: Dataprotectieverdrag.

¹⁶ www.CBPweb.nl → over het CBP.

¹⁷ www.CBPweb.nl → Over CBP → Organisatie → Bestuur en beleid → bestuursreglement.

¹⁸ Art. 5:21 Awb.

geregeld in de Awb.¹⁹ Verder geeft de Awb de bevoegdheid aan het orgaan dat bevoegd is tot een last onder bestuursdwang, in plaats daarvan te kiezen voor een last onder dwangsom.²⁰ Deze last onder dwangsom beschrijft de herstelmaatregelen die moeten worden genomen en er wordt een termijn gesteld waarbinnen de overtreder de onrechtmatige situatie moet herstellen.²¹

Naast de last onder bestuursdwang en de last onder dwangsom heeft het CBP bij bepaalde overtredingen de bevoegdheid om een bestuurlijke boete op te leggen. Het gaat dan om overtredingen op het verplicht melden van verwerkingen van persoonsgegevens. Dit zijn het ten onrechte achterwege laten van de melding, het achterwege laten van een melding van een niet-geautomatiseerde verwerking voor zover onderworpen aan een voorafgaand onderzoek, het starten van de verwerking alvorens de melding heeft plaatsgevonden, het doen van een onvolledige melding, het achterwege laten van de melding het doel of de doeleinden waarvoor de gegevens of de categorie gegevens zijn verzameld, het niet of niet tijdig doorgeven van wijzigingen van de eerder gemelde gegevens en het niet vastleggen of bewaren van een specifieke categorie van verwerkingen.²²

De hoogte van de bestuurlijke boete is maximaal 4500 euro.²³ In de Wbp wordt verwezen naar beleidsregels die opgesteld zijn door de minister.²⁴ In de Beleidsregels handhaving door het CBP staat dat de inzet van handhavingsinstrumenten door het CBP af hangt van de omstandigheden van het geval, waaronder de inhoud van en de strekking van de overtreden norm en de daarbij betrokken belangen. Doel, effect en efficiëntie staan voorop. Hieruit blijkt dat deze overwegingen worden betrokken bij de keuze voor een handhavingsinstrument maar ook bij de hoogte van de boete.²⁵

4.4 De toegang tot het digitaal cliëntdossier

Het CBP heeft afgelopen zomer een rapport uitgebracht waarin de resultaten van een onderzoek naar de toegang tot digitale patiëntdossier binnen zorginstellingen worden gepresenteerd. Uit het rapport kwam naar voren dat zorginstellingen waar geen logging plaatsvindt van alle acties, niet voldoen aan art. 13 Wbp.²⁶ De controle op de logging is ook een wettelijk vereiste. Het CBP gaf aan in haar rapport dat zorginstellingen waar geen systematische controle van alle logging plaatsvindt, derhalve niet voldoen aan artikel 13 Wbp.²⁷ In art. 13 Wbp staat dat de verantwoordelijke passende en technische maatregelen ten uitvoer moet leggen om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Het CBP geeft ten slotte aan in haar rapport dat voor het voldoende beveiligen van persoonsgegevens gebruik gemaakt kan worden van de Code voor Informatiebeveiliging en NEN 7510. Dit zijn beveiligstandaarden die het hele terrein van de informatiebeveiliging binnen een organisatie afdekken. Wanneer men aan deze standaarden voldoet, voldoet men ook aan de plicht uit het Wbp om technische en organisatorische maatregelen te implementeren.

¹⁹ Afdeling 5.2 Awb.

²⁰ Art. 5:32 Awb.

²¹ Art. 5:32a Awb.

²² Art. 27 lid 1,2,3 jo. 28 lid 1,3,4 Wbp.

²³ Art. 66 Wbp.

²⁴ Art. 74 Wbp.

²⁵ Art. 3.1 onder e Beleidsregels handhaving door het CBP.

²⁶ *Toegang tot digitale cliëntendossiers binnen zorginstellingen* (rapport van het CBP), Den Haag: juni 2013.

²⁷ *Toegang tot digitale cliëntendossiers binnen zorginstellingen* (rapport van het CBP), Den Haag: juni 2013, p. 8.

Uit een gesprek met het CBP is daarnaast naar voren gekomen dat wanneer er sprake is van een cliëntdossier waar ook medische gegevens in staan, dit dossier extra beveiligd dient te worden. Dit is mogelijk met een twee factor authenticatie. Twee factor authenticatie houdt in dat er gebruik wordt gemaakt van twee soorten beveiligingen. Bijvoorbeeld zowel een kennis beveiliging, een wachtwoord, en een fysieke beveiliging, bijvoorbeeld een pas of sleutel die moet worden ingevoerd.

4.5 Delen van persoonsgegevens in samenwerkingsverband

Het CBP heeft een informatieblad opgesteld over het delen van informatie in samenwerkingsverbanden. De onderstaande informatie in deze paragraaf is afkomstig uit het informatieblad van het CBP.²⁸ Hieronder wordt besproken wat het CBP aangeeft als belangrijkste punten om bij stil te staan wanneer men gegevens wil delen in samenwerkingsverband.

Gemeenschappelijk doel

Het CBP geeft aan dat het noodzakelijk is om een gemeenschappelijk doel vast te stellen met betrekking tot het delen van de gegevens. De Wbp schrijft voor dat persoonsgegevens alleen mogen worden verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Het doel waarvoor de gegevens worden verzameld en vervolgens gebruikt, is bepalend voor de hoeveelheid en de soort informatie die mag worden gedeeld. Voor het delen van medische en strafrechtelijke gegevens gelden strengere regels. Deze gegevens mogen alleen gedeeld worden wanneer de wet dit uitdrukkelijk toestaat.

Grondslag

Verder is het belangrijk dat er een grondslag is voor het delen van de persoonsgegevens. De reden hiervoor, is dat het delen van persoonsgegevens ook onder het verwerken van gegevens valt en dat uit de wet voort vloeit dat verwerken van gegevens alleen is toegestaan wanneer daar een wettelijke grondslag voor is zoals genoemd in de Wbp.²⁹ De toestemming van de betrokkene zal hier vaak geen grondslag zijn. De reden die het CBP hiervoor geeft is dat het initiatief tot samenwerking niet van de betrokkene afkomstig zal zijn en diegene vaak afhankelijk is van de partijen die samenwerken.

Verenigbaar

Voordat gegevens worden gedeeld binnen een samenwerkingsverband moet worden beoordeeld of het doel waarvoor de informatie gedeeld wordt, verenigbaar is met het doel waarvoor de gegevens oorspronkelijk zijn verzameld. Het CBP heeft daarbij een aantal dingen opgemerkt.

- Hoe dichter de twee doeleinden bij elkaar liggen, hoe eerder het verdere gebruik van gegevens verenigbaar zal zijn.
- Als de betrokkene de gegevens als gevoelig ervaart, mag minder snel aangenomen worden dat de gegevens ook voor andere doeleinden mogen worden gebruikt. Een voorbeeld van gevoelige gegevens zijn inkomensgegevens.

²⁸ *Informatie delen in samenwerkingsverband* (informatieblad van het CBP), februari 2012.

²⁹ Art. 8 Wbp.

- Wanneer het verdere gebruik van gegevens tot gevolg heeft dat een bepaalde beslissing over de betrokkene wordt genomen, moet er een extra afweging gemaakt worden. Het voorbeeld dat hierbij wordt genoemd is wanneer het gebruik ertoe leidt dat de betrokkene wordt beperkt in zijn mogelijkheden om zich maatschappelijk te ontwikkelen zoals bij een verslaafde die een gebiedsontzegging krijgt opgelegd.

Omvang

De omvang van de gegevens die gedeeld mogen worden, is onder meer afhankelijk van het doel waarvoor de gegevens gedeeld worden. Als voorbeeld wordt gegeven de bemoeizorg. Het doel bij bemoeizorg is om de cliënt naar de reguliere hulpverlening te geleiden. Er wordt daar onderscheid gemaakt in ketenpartners en schilpartners. De ketenpartners zijn de partners die direct betrokken zijn bij de behandeling/begeleiding van de cliënt. De schilpartners zullen niet bij elke overleg en bij elke casus aanwezig hoeven zijn. Dit kunnen bijvoorbeeld politie, woningcorporaties, gemeente of andere hulpverleners zijn. Zowel de ketenpartners als de schilpartners wisselen alleen de hoogstnoodzakelijke gegevens uit.

Geheimhoudingsplicht

Door het medisch beroepsgeheim is het meestal niet mogelijk om het medisch dossier ter beschikking te stellen aan bijvoorbeeld politie of justitie. Hier wordt ook het mondeling delen of het laten meekijken via een computerscherm onder gerekend. De geheimhoudingsplicht kan in sommige gevallen doorbroken worden. Bijvoorbeeld wanneer iemand toestemming geeft voor het delen van zijn gegevens. Wanneer deze toestemming niet wordt gegeven maar de hulpverlener is van mening dat het delen van de gegevens noodzakelijk is, kan in uitzonderingssituaties buitenkant informatie gedeeld worden. Dit zijn de hoogstnoodzakelijke gegevens. Het voorbeeld dat gegeven wordt is wanneer de GGD aan een woningcorporatie niet mag laten weten dat een persoon gediagnosticeerd is met schizofrenie. Wanneer dit wel noodzakelijk is om te laten weten, om overlast te voorkomen of bestrijden, kan de GGD laten weten dat er kans is op onvoorspelbaar impulsief agressief gedrag. Ook kan het noodzakelijk zijn om de woningcorporatie te informeren dat de betrokkene onder behandeling is en de geconstateerde problemen zullen afnemen.

stappenplan

Het informatieblad van het CBP geeft daarnaast een stappenplan dat kan worden gevolgd bij het delen van informatie in samenwerkingsverband. Dit zijn de genoemde stappen:

1. bepaal de taken en belangen;
2. bepaal het doel van het delen van informatie;
3. bepaal welke gegevens u deelt;
4. bepaal de vorm en inhoud van het delen;
5. bepaal de verantwoordelijke en maak afspraken;
6. maak afspraken over hoe en wanneer u de betrokkenen van informatie voorziet.

4.6 Slot

Het CBP voert een aantal taken uit, namelijk; toezicht houden, adviseren, geven van voorlichting en informatie verstrekken. Ook hebben ze hebben internationale taken. De controle op het CBP gebeurt vanuit de wet en is daarnaast mogelijk door de burger. Het Cbp kan verschillende sancties opleggen, waaronder bestuursdwang en een bestuurlijke boete. Het CBP geeft aan dat logging van alle acties in een digitaal cliëntdossier een verplichting is die voortvloeit uit de Wbp, evenals een regelmatige controle op deze logging. Gegevens moeten goed worden beschermd en het CBP geeft aan dat voor een juiste bescherming van persoonsgegevens gebruik gemaakt kan worden van de Code voor Informatiebeveiliging en NEN 7510. Als het gaat om medische gegevens moeten deze extra worden beschermd, bijvoorbeeld door een twee factor authenticatie. Wanneer gegevens gedeeld worden in samenwerkingsverband moet op een aantal punten gelet worden en kan bij het maken van samenwerkingsafspraken gebruik gemaakt worden van het informatieblad dat is opgesteld door het CBP.

Hoofdstuk 5. De juridische grenzen

Het recht op privacy is verbonden met het beroepsgeheim. Normen met betrekking tot het beroepsgeheim werken door in het recht op privacy. Daar waar het beroepsgeheim betrekking heeft op de relatie van patiënten met individuele beroepsbeoefenaren, heeft het privacyrecht betrekking op persoonsgegevens die buiten de eigen administratie van de beroepsbeoefenaar wordt opgeslagen en door anderen wordt beheerd. Het verzamelen en opslaan van persoonsgegevens in (vaak) geautomatiseerde systemen houdt een specifieke bedreiging in van de persoonlijke levenssfeer en het is daarom belangrijk dat hier regels over gesteld zijn. Het is namelijk moeilijk controleerbaar wat er over een persoon wordt vastgelegd en hoe met die gegevens om wordt gegaan. Op basis van deze gegevens worden daarnaast vaak beslissingen genomen en is de juistheid van deze gegevens van groot belang. Een derde reden voor het belang van privacyregels is dat derden geregeld de beschikking willen over de gegevens voor eigen doeleinden. Beperking van de mogelijkheid om kennis te nemen van de gegevens is een belangrijk onderdeel van informationele privacybescherming. Hierbij is niet alleen de externe toegang van belang, ook binnen instellingen moet deze privacybescherming worden bewaakt.³⁰

In dit hoofdstuk zullen de verschillende rechtsbronnen die van toepassing zijn op de privacy van instellingen met zorggegevens besproken worden. In paragraaf 1 worden, om de achtergrond van de nationale wetgeving te geven, internationale overeenkomsten, verklaringen en aanbevelingen besproken, in paragraaf 2 komen de Wet bescherming persoonsgegevens en de regeling van de geneeskundige behandelingsovereenkomst in het burgerlijk wetboek (WGBO) aan de orde. Hier zal worden uitgewerkt welke eisen deze regelingen geven aan de verantwoordelijke en welke rechten aan de betrokkene. Vervolgens zal in paragraaf 3 de toekomstige Algemene Verordening Gegevensbescherming worden toegelicht en welke gevolgen deze verordening heeft voor Traverse. Ten slotte wordt het hoofdstuk afgesloten met een conclusie in paragraaf 4.

5.1 Het internationaal juridische kader

5.1.1 Inwerking treden van bepalingen uit internationale verdragen

Nederland is een monistische staat. Dit houdt in dat Nederland de automatische interne werking van internationaal publiekrecht heeft aanvaard. Zodra een regel van internationaal recht op internationaal niveau verbindend wordt verklaard, wordt deze regel deel van de nationale rechtsorde.³¹

In de grondwet zijn artikelen opgenomen die vastleggen dat internationale regelingen werking hebben in het nationale recht. De Grondwet geeft weer dat bepalingen van verdragen en besluiten van volkenrechtelijke organisaties, die naar inhoud een ieder kunnen verbinden, verbindende kracht hebben nadat zij zijn bekendgemaakt.³² In de grondwet staat verder dat wanneer nationale regelgeving in strijd is met een ieder

30 H.J.J. Leenen, J.K.M. Gevers & J. Legemaate, *Handboek gezondheidsrecht. Deel 1. Rechten van mensen in de gezondheidszorg*, Den Haag: Boom Juridische uitgevers 2012, p. 252.

31 A. Nollkaemper, *Kern van het internationaal publiekrecht*, Den Haag: Boom Juridische uitgevers 2011, p. 488-489.

32 Art. 93 Gw.

verbindende bepaling van verdragen en van besluiten van volkenrechtelijke organisaties de nationale regelgeving niet geldig is.³³

Een ieder verbindende bepaling, zoals dit in de Grondwet genoemd wordt, is een bepaling die verbindende kracht heeft jegens burgers.³⁴ Ook bepalingen die slechts betekenis hebben voor één persoon of een gesloten kring van personen kunnen een iedere verbindend zijn.³⁵ Wanneer een bepaling een ieder verbindend is, kan de burger aanspraak maken op deze bepaling en dient hij toepassing ervan accepteren, ook als daarmee zijn rechtspositie wordt aangetast. Afhankelijk van de inhoud van de bepaling kan het door de overheid aan de burger, door de burger aan de overheid of door de ene burger aan de andere burger worden tegengeworpen.³⁶

Met bepalingen die een ieder kunnen verbinden worden bepalingen bedoeld die self-executing zijn. Een bepaling is self-executing als deze vatbaar is voor rechtstreekse toepassing door bestuur en er dus geen verdere wettelijke voorschriften hoeven worden vastgesteld om tenuitvoerlegging mogelijk te maken.³⁷

5.1.2 Gezondheidsrecht en recht op privacy in Internationale verdragen

Internationaal zijn verschillende ontwikkelingen van belang geweest op het gebied van patiëntenrechten met betrekking tot privacy. De Universele verklaring van de rechten van de mens van 1948 en het Internationaal verdrag inzake burgerrechten en politieke rechten (IVBPR) van 1966, beide van de Verenigde Naties, bevatten ondermeer bepalingen die strekken tot bescherming van de persoonlijke levenssfeer.³⁸ Ook het Europese Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden bevat bepalingen inzake de bescherming van de persoonlijke levenssfeer.^{39 40}

In het UVRM en IVBPR is opgenomen dat niemand mag worden onderworpen aan willekeurige of onwettige inmenging in zijn privé leven, zijn gezinsleven, zijn huis en zijn briefwisseling, noch aan onwettige aantasting van zijn eer en goede naam en dat een ieder recht heeft op bescherming door de wet tegen zodanige inmenging of aantasting.⁴¹ In het EVRM is tevens opgenomen dat een ieder heeft recht op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.

5.2 Het nationaal juridisch kader

5.2.1 De Wet bescherming persoonsgegevens

5.2.1.1 Achtergrond

De Wbp geeft uitvoering aan een Europese richtlijn uit 1995. Kort gezegd geeft de Wbp weer hoe er met persoonsgegevens om dient te worden gegaan. Zoals in de vorige paragraaf omschreven is, is het recht op bescherming van de persoonlijke levenssfeer gewaarborgd in

33 Art. 94 Gw.

34 Art. 93 Gw.

35 Art. 94 jo. 94 Gw.

36 P.P.T. Bovend'Eert e.a., *Grondwet voor het Koninkrijk der Nederlanden*. Tekst en commentaar, Deventer: Kluwer 2009.

37 P.P.T. Bovend'Eert e.a., *Grondwet voor het Koninkrijk der Nederlanden*. Tekst en commentaar, Deventer: Kluwer 2009.

38 Art. 12 UVRM jo. art. 17 IVBPR.

39 *Kamerstukken II* 1989/90, 21 561, nr 3 (MvT).

40 Art. 8 EVRM.

41 Art. 17 IVBPR.

het EVRM en in het IVBPR.^{42 43} De term ‘privé leven’ zoals die in deze verdragen gebruikt wordt, heeft dezelfde betekenis als de term ‘persoonlijk levenssfeer’ in de Grondwet. Naast art. 8 EVRM geeft de Wbp ook uitvoering aan het Verdrag inzake gegevensbescherming.⁴⁴ In onderstaand schema is te zien op grond van welke voorgaande regelingen uiteindelijk de Wbp tot stand is gekomen. Daarnaast is vast de toekomstige Algemene Verordening Gegevensbescherming toegevoegd aan het schema.

Datum	Regeling
1976	Eindrapport van Staatscommissie – Koopmans
1981	Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (Europees Dataverdrag)
1983	Artikel 10 Grondwet
1989	Wet persoonsregistratie
1995	Europese richtlijn betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens
2001	Wet bescherming persoonsgegevens
-	Algemene Verordening Gegevensbescherming

Door de in de jaren 70 opkomende computertechnologie ontstond er maatschappelijke onrust. Er konden grote hoeveelheden persoonsgegevens worden opgeslagen en verwerkt en daardoor vreesden veel mensen dat de controle op burgers door de overheid te groot zou worden. Naar aanleiding van deze onrust stelde de regering een commissie in. Deze commissie had als opdracht onderzoek te verrichten naar de mogelijkheden om de verwerking van persoonsgegevens te reguleren via een wettelijke regeling. Het doel van deze regeling was het beschermen van de persoonlijke levenssfeer. In de eindrapportage van het onderzoek had de commissie een voorontwerp voor de Wet op de Persoonsregistratie opgenomen.⁴⁵ In 1981 werd dit voorontwerp als wetsvoorstel aan de Tweede Kamer gestuurd. In 1981 werd ook het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens getekend. Bovenstaande ontwikkelingen hebben er toe geleid dat in 1983 het recht op bescherming van de persoonlijke levenssfeer in de Grondwet werd opgenomen.^{46 47}

In de Grondwet staat dat de wet regels stelt ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens en dat de wet regels stelt inzake de aanspraken van personen op kennisneming van over hen vastgelegde

⁴² Art.8 EVRM.

⁴³ Art. 17 IVBPR.

⁴⁴ *Kamerstukken II 1997/98, 25 892, nr 3 (MvT).*

⁴⁵ Staatscommissie Koopmans, *Eindrapport van de Staatscommissie bescherming persoonlijke levenssfeer in verband met persoonsregistratie*, Den Haag: 1976.

⁴⁶ Art. 10 Gw.

⁴⁷ W.I. Koelewijn, *Privacy en politiegegevens. Over geautomatiseerde normatieve informatieuitwisseling*, Leiden: Leiden University Press 2009, p.56-57.

gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.⁴⁸

Artikel 10

- 1.**Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.
- 2.**De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.
- 3.**De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.

In dit artikel staat dat de wet regels stelt ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens en dat de wet regels stelt inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.⁴⁹

Lid 2 van art. 10 GW geeft aan dat de wet regels moet stellen ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens. In 1989 is de Wet persoonsregistratie ingevoerd en deze wet geeft daarmee uitvoering aan het gestelde uit art.10 lid 2 GW.

Richtlijn 95/46/EG ofwel de Europese richtlijn betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, werd in 1995 vastgesteld. Deze richtlijn had twee doelstellingen namelijk: het fundamentele recht op gegevensbescherming waarborgen en het vrije verkeer van persoonsgegevens tussen de lidstaten garanderen. Deze privacyrichtlijn uit oktober 1995 had uiterlijk drie jaar later in wetgeving moeten zijn omgezet.⁵⁰ Dit is echter pas gebeurd in 2001. Toen is de Wet bescherming persoonsgegevens als uitvoering van de Europese richtlijn tot stand gekomen. In de nabije toekomst zal de Algemene Verordening gegevensbescherming in werking treden, deze verordening wordt toegelicht in paragraaf 5.3.

5.2.1.2 Reikwijdte van de Wbp

De reikwijdte is uitgewerkt in de Wbp. Hierin staat dat de wet van toepassing is op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen. Belangrijke begrippen die naar voren komen uit dit artikel om de reikwijdte af te kunnen bakenen zijn 'persoonsgegeven', 'verwerken', en 'bestand'. Deze begrippen zullen nu verder worden toegelicht.

Een van de begrippen uit de Wbp is 'persoonsgegevens'.⁵¹ In art. 1 Wbp staat wat onder persoonsgegevens wordt begrepen: elk gegeven betreffende een geïdentificeerde of

⁴⁸ Art. 10 lid 2 en 3 Gw.

⁴⁹ Art. 10 lid 2 en 3 Gw.

⁵⁰ P.J. Hustinx, *Nederland moet Europese privacy-richtlijn volgen* (artikel gepubliceerd op cbp.nl), augustus 1999.

⁵¹ Art.2 Wbp.

identificeerbare natuurlijke persoon.⁵² Een gegeven is niet herleidbaar als er een onevenredige hoeveelheid tijd, geld en mankracht nodig is om herleiding tot een individuele persoon mogelijk te maken.⁵³ Persoonsgegevens kunnen worden onderverdeeld in algemene persoonsgegevens en bijzondere persoonsgegevens.

Onder het verwerken van gegevens wordt door de Wbp verstaan: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.⁵⁴ In hoofdstuk 2 van de Wbp worden eisen gesteld aan het verwerken van persoonsgegevens. Deze voorwaarden zijn:

- Persoonsgegevens moeten in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze worden verwerkt.⁵⁵
- Persoonsgegevens moeten voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld.⁵⁶
- Persoonsgegevens mogen alleen worden verwerkt indien het een grondslag heeft die in de Wbp genoemd staat.⁵⁷
- Persoonsgegevens mogen niet verder verwerkt worden op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.⁵⁸ Om te kunnen beoordelen of een verwerking onverenigbaar is moet rekening gehouden worden met:
 - De verwantschap tussen het doel van de beoogde verwerking en het doel waarvoor de gegevens zijn verkregen.
 - De aard van de betreffende gegevens.
 - De gevolgen van de beoogde verwerking voor de betrokkene.
 - De wijze waarop de gegevens zijn verkregen.
 - De mate waarin jegens de betrokkene wordt voorzien in passende waarborgen.
- Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt.⁵⁹
- Persoonsgegevens mogen slechts worden verwerkt voor zover zij toereikend, ter zake dienend en niet bovenmatig zijn.

De Wbp geeft aan dat de verwerking van bijzondere persoonsgegevens verboden is. Onder bijzondere persoonsgegevens vallen godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging en strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd

⁵² Art.1 Wbp.

⁵³ H.J.J. Leenen, J.K.M. Gevers & J. Legemaate, *Handboek gezondheidsrecht. Deel 1. Rechten van mensen in de gezondheidszorg*, Den Haag: Boom Juridische uitgevers 2012, p.254.

⁵⁴ Art. 1 sub b Wbp.

⁵⁵ Art. 6 Wbp.

⁵⁶ Art. 7 Wbp.

⁵⁷ Art. 8 Wbp.

⁵⁸ Art. 9 Wbp.

⁵⁹ Art. 10 Wbp.

verbod naar aanleiding van dat gedrag. Verwerking van deze gegevens is dus verboden tenzij er een uitzondering van toepassing is. Deze uitzonderingen zijn opgenomen in de Wbp.⁶⁰ Belangrijk is wel dat de verwerking alleen toegestaan is 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.

In de handleiding wet bescherming persoonsgegevens staan een aantal nuttige schema's waaronder een schema over rechtmatige verwerking.⁶¹ Door deze af te lopen wordt duidelijk of op een rechtmatige manier persoonsgegevens worden verwerkt. Deze schema's zijn opgenomen in de bijlage.

Een ander belangrijk begrip uit de Wbp is 'persoonsgegevens'.⁶² Onder persoonsgegevens wordt begrepen: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. Een gegeven is niet herleidbaar als er een onevenredige hoeveelheid tijd, geld en mankracht nodig is om herleiding tot een individuele persoon mogelijk te maken.⁶³

Het laatste begrip is 'bestand'. In de Wbp wordt bestand gedefinieerd als: elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen. Uit jurisprudentie is gebleken dat een boek door toevoeging van een persoonsregister kan worden aangemerkt als een bestand.⁶⁴ Een dossier over het functioneren van een medisch specialist is geen bestand als bedoeld in de Wbp.⁶⁵ Het enkele feit dat het dossier chronologisch geordend is, kan niet tot de conclusie leiden dat sprake is van een gestructureerd geheel van persoonsgegevens dat volgens bepaalde criteria toegankelijk is. Het dossier maakt evenmin deel uit van een ander bestand.^{66 67}

5.2.1.3 Plichten van de verantwoordelijke

Een verantwoordelijke in de zin van de Wbp is een natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Aan deze verantwoordelijke wordt door de Wbp verplichtingen gesteld. Deze verplichten worden hierna uitgewerkt.

Geheimhoudingsplicht

In de Wbp is geregeld dat personen die gegevens verwerken geheimhoudingsplicht hebben ten aanzien van de gegevens die ze verwerken. Dit geldt slechts voor wie nog niet uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht geldt.⁶⁸

⁶⁰ Art. 17 t/m 23 Wbp.

⁶¹ L.B. Sauerwein & J.J. Linneman, *Handleiding voor verwerkers van persoonsgegevens*, Den Haag: Ministerie van Justitie 2002, p.8.

⁶² Art. 2 Wbp.

⁶³ H.J.J. Leenen, J.K.M. Gevers & J. Legemaate, *Handboek gezondheidsrecht. Deel 1. Rechten van mensen in de gezondheidszorg*, Den Haag: Boom Juridische uitgevers 2012, p.254.

⁶⁴ Rb. Amsterdam 23 oktober 2012, *LJN* BY0934.

⁶⁵ Art. 1 sub c Wbp.

⁶⁶ HR 3 juni 2005, *LJN* AT1093.

⁶⁷ www.CBPweb.nl → Wbp-naslag → Hoofdstuk 1 Algemene bepalingen → art. 1 sub c Wbp.

⁶⁸ Art. 12 lid 2 Wbp.

Melden

De verantwoordelijke heeft als plicht gegevensverwerking te melden bij het college bescherming persoonsgegevens of wanneer een functionaris voor de gegevensbescherming is benoemd, bij deze functionaris.^{69 70}

Een functionaris van de gegevensbescherming is een interne toezichthouder die benoemd kan worden door Traverse, de brancheorganisatie of een organisatie waarbij meerdere verantwoordelijke zijn aangesloten. Een functionaris kan alleen een natuurlijke persoon zijn die de wettelijke taken en de bevoegdheden op zich neemt. Dit kan dus niet een gehele privacycommissie zijn. Zoals aangegeven is het gevolg van het benoemen van een privacyfunctionaris voor de gegevensbescherming, dat de verplichte melding nu intern plaats kan vinden bij de functionaris in plaats van bij het college bescherming persoonsgegevens. Er zijn een paar eisen gesteld aan deze functionaris. Deze persoon moet over voldoende kennis beschikken over de privacyregelgeving van de organisatie, en van de gegevensverwerking binnen deze organisatie. Daarnaast moet de persoon voldoende betrouwbaar zijn. Wanneer een functionaris benoemd is kan hem wat betreft zijn taken als functionaris van de gegevensbescherming geen aanwijzingen meer gegeven worden. Hij moet zijn taken onafhankelijk kunnen uitvoeren en hij moet bevoegdheden krijgen om zijn taak uit te kunnen voeren die gelijk staan aan de bevoegdheden van het CBP. Deze bevoegdheden zijn onder andere ruimtes betreden, inlichtingen vragen en inzage vorderen in gegevens en stukken. De functionaris moet erop toezien dat gegevens in overeenstemming met de wet worden verwerkt. Verder houdt hij een register met de meldingen bij en stelt ieder jaar een verslag van zijn werkzaamheden en bevindingen op. De functionaris kan in dit verslag maar ook daarbuiten aanbevelingen doen om de bescherming van gegevens te verbeteren en kan hiertoe overleggen met het CBP.⁷¹

Wanneer persoonsgegevens worden verwerkt moet dit worden gemeld. Het gaat dan om geheel of gedeeltelijk geautomatiseerde gegevensverwerking en handmatige gegevensverwerking. Een handmatige gegevensverwerking hoeft in beginsel niet te worden gemeld. Dit is anders wanneer de handmatige gegevensverwerking is onderworpen aan een voorafgaand onderzoek. De wetgever heeft een aantal gegevensverwerkingen benoemd die aan het voorafgaand onderzoek zijn onderworpen. Het gaat dan om verwerkingen die volgens de wetgever een grote inbreuk op de persoonlijke levenssfeer van de betrokkene betekenen.⁷² De betrokkene wordt door de Wbp als volgt gedefinieerd: degene op wie een persoonsgegeven betrekking heeft.

In de Wbp is een aantal verwerkingen genoemd die niet gemeld hoeven te worden. Deze vrijgestelde gegevensverwerkingen worden opgesomd in het vrijstellingsbesluit.

⁶⁹ L.B. Sauerwein & J.J. Linneman, *Handleiding voor verwerkers van persoonsgegevens*, Den Haag: Ministerie van Justitie 2002, p. 30.

⁷⁰ Art. 27 Wbp.

⁷¹ L.B. Sauerwein & J.J. Linneman, *Handleiding voor verwerkers van persoonsgegevens*, Den Haag: Ministerie van Justitie 2002, p.44-46.

⁷² L.B. Sauerwein & J.J. Linneman, *Handleiding voor verwerkers van persoonsgegevens*, Den Haag: Ministerie van Justitie 2002, p 29-31.

Beveiligen gegevens

De Wbp verplicht de verantwoordelijke om de gegevensverwerking te beveiligen.⁷³ De Wbp vermeldt dat er passende technische en organisatorische maatregelen genomen moeten worden om het verlies of onrechtmatige verwerking tegen te gaan. Deze maatregelen moeten een passend beveiligingsniveau garanderen gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen. Er wordt met de maatregelen rekening gehouden met de stand van de techniek en de kosten van de tenuitvoerlegging. De Wbp bevat geen concrete normen voor beveiliging. In de praktijk zijn hier standaarden voor ontwikkeld. Voor de zorgsector is met name van belang de nadere uitwerking van de Code voor Informatiebeveiliging in de standaard NEN 7510. In de publicatie Richtsnoeren beveiliging van persoonsgegevens van het CBP staan aanbevelingen om ter bepaling van hetgeen in een concrete situatie passend is in de zin van de Wbp, gebruik te maken van algemeen geaccepteerde beveiligingsstandaarden.⁷⁴ De NEN 7510 is een gezaghebbende sectorale uitwerking van artikel 13 Wbp. Als een ziekenhuis voldoet aan NEN 7510 mag ervan uit worden gegaan dat het ook voldoet aan de Wbp. Een ziekenhuis kan ook op andere wijze aantonen dat de beveiliging op orde is, bijvoorbeeld door te voldoen aan de Code voor Informatiebeveiliging. Wanneer het CBP beveiligingsmaatregelen van zorginstellingen toetst aan de Wbp gebruikt het CBP de NEN 7510.⁷⁵ De Code voor informatiebeveiliging en NEN 7510 zijn beveiligingsstandaarden die het hele terrein van de informatiebeveiliging binnen een organisatie afdekken.⁷⁶

Bewaren van gegevens

In de Wbp is opgenomen dat persoonsgegevens niet langer mogen worden bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren dan noodzakelijk is voor de verwerking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt.⁷⁷ Hoe lang de gegevens bewaard mogen worden is dus afhankelijk van het doel waarvoor de gegevens zijn verzameld en verwerkt. Wanneer het voor het doel niet meer noodzakelijk is de gegevens te bewaren dienen ze te worden verwijderd of moet er voor worden gezorgd dat de betrokkene niet meer te identificeren is door alle identificerende kenmerken te verwijderen.⁷⁸

Voor van de meldingsplicht vrijgestelde gegevensverwerkingen kan een maximale bewaartermijn zijn opgenomen in het Vrijstellingsbesluit. Ook in andere specifieke wetten kunnen maximale bewaartermijnen zijn opgenomen. In de Wbp staat slechts dat de gegevens niet langer mogen worden bewaard dan noodzakelijk is voor het doel waarvoor de gegevens verzamelt of verder verwerkt worden. In het Vrijstellingsbesluit Wbp is opgenomen dat instellingen inzake gezondheidszorg persoonsgegevens dienen te verwijderen, uiterlijk

⁷³ Art. 13 jo. 14 Wbp.

⁷⁴ Art. 13 Wbp.

⁷⁵ Art. 13 Wbp.

⁷⁶ *Toegang tot digitale cliëntendossiers binnen zorginstellingen* (rapport van het CBP), Den Haag: juni 2013.

⁷⁷ Art. 10 Wbp.

⁷⁸ L.B. Sauerwein & J.J. Linneman, *Handleiding voor verwerkers van persoonsgegevens*, Den Haag: Ministerie van Justitie 2002, p.40.

vijf jaar nadat de verlening van zorg is geëindigd, tenzij de persoonsgegevens noodzakelijk zijn ter voldoening aan een wettelijke bewaarplicht.⁷⁹

Informatieplicht

In de Wbp is verder de informatieplicht geregeld.⁸⁰ In deze artikelen staat dat indien persoonsgegevens worden verkregen bij de betrokkene, de verantwoordelijke vóór het moment van de verkrijging de betrokkene de informatie mededeelt tenzij de betrokkene daarvan op de hoogte is. Het is niet genoeg wanneer de verantwoordelijke vermoedt dat de betrokkene op de hoogte is, de verantwoordelijke moet zeker weten dat dit het geval is. Wanneer de verantwoordelijke de informatie verzonden of uitgereikt heeft mag deze ervan uitgaan dat de betrokkene op de hoogte is. Wanneer uit een gedraging of een verklaring van de betrokkene naar objectieve maatstaven kan worden afgeleid dat de betrokkene op de hoogte is mag hier ook van worden uitgegaan. Naar objectieve maatstaven houdt in dat iedereen uit de gedragingen zou afleiden dat de betrokkene op de hoogte is. De verantwoordelijke mag er niet vanuit gaan dat de betrokkene op de hoogte is, wanneer deze persoon op de hoogte had kunnen zijn. Ook wanneer de betrokkene bijvoorbeeld door onderzoek zou kunnen achterhalen wie de verantwoordelijke is en voor welke doeleinden de gegevens worden verwerkt, moet de betrokkene door de verantwoordelijke worden geïnformeerd. De informatie die verstrekt moet worden op grond van de Wbp is in ieder geval de naam van de verantwoordelijke en voor welk doel of doeleinde de gegevens worden verzameld en verwerkt.⁸¹ Verder is opgenomen dat de verantwoordelijke nadere informatie verstrekt aan de betrokkene wanneer dit gelet op de aard van de gegevens, de omstandigheden waaronder zij worden verkregen of het gebruik dat ervan wordt gemaakt, nodig is om tegenover de betrokkene een behoorlijke en zorgvuldige verwerking te waarborgen.⁸² En zoals eerder is omschreven is een zorgvuldige en behoorlijke verwerking op grond van de Wbp een voorwaarde voor verwerking van persoonsgegevens. Hoe gevoeliger de gegevens die worden verwerkt voor de betrokkene liggen, hoe meer reden er is om de betrokkene gedetailleerd te informeren over de gegevensverwerking.⁸³

Het moment van informeren is afhankelijk van de wijze van verkrijging van de gegevens. Wanneer de verantwoordelijke de gegevens van de betrokkene zelf krijgt moet de betrokkene vóór het verkrijgen van de gegevens worden geïnformeerd. Wanneer de verantwoordelijke de gegevens verkrijgt buiten de betrokkene om moet de betrokkene worden geïnformeerd op het moment dat de gegevens worden vastgelegd. Wanneer de gegevens uitsluitend worden verzameld om deze aan een derde te verstrekken moet de betrokkene uiterlijk op het moment van eerste verstrekking aan die derde worden geïnformeerd.⁸⁴

De informatie moet op zodanige wijze worden verstrekt aan de betrokkene zodat deze er daadwerkelijk de beschikking over heeft. Wanneer de gegevens zijn verkregen van de

⁷⁹ Art. 17 Vrijstellingsbesluit Wbp.

⁸⁰ Art. 33 jo. 34 Wbp.

⁸¹ Art. 33 lid 2 Wbp.

⁸² Art. 33 lid 3 Wbp.

⁸³ L.B. Sauerwein & J.J. Linneman, *Handleiding voor verwerkers van persoonsgegevens*, Den Haag: Ministerie van Justitie 2002, p. 33-34.

⁸⁴ L.B. Sauerwein & J.J. Linneman, *Handleiding voor verwerkers van persoonsgegevens*, Den Haag: Ministerie van Justitie 2002, p. 34-35.

betrokkene zelf dan kan de informatie bijvoorbeeld opgenomen worden op het formulier waarop de betrokkene de gegevens verstrekt. Een andere mogelijkheid is een folder of brochure aan de betrokkene uitreiken of toesturen. Zoals hierboven uitgelegd is moet dit wel gebeuren voordat de betrokkene de gegevens verstrekt. Wanneer de gegevens via een andere weg verkregen worden dan moet er gekeken worden of het om een beperkt aantal betrokkene gaat of om een hele groep. In het eerste geval moeten de betrokkene persoonlijk worden geïnformeerd. In het tweede geval mag worden volstaan met een algemenere vorm van informatieverstrekking. Hierbij kan worden gedacht aan een blad of tijdschrift, maar er moet wel vaststaan dat daarmee de hele groep van betrokkene wordt bereikt. Een advertentie in een landelijk dagblad of een huis-aan-huisblad is niet voldoende.⁸⁵

Er hoeft niet te worden geïnformeerd wanneer de informatieverstrekking onmogelijk is of alleen met onevenredige inspanning kan plaatsvinden. Hiervan in sprake wanneer alleen door een zeer tijdrovende inspanning het adres van betrokkene kan worden achterhaald. In zo'n geval moet de herkomst van de gegevens worden vastgelegd zodat de betrokkene in ieder geval achteraf kan nagaan welke weg de gegevens hebben afgelegd. Er hoeft ook niet te worden geïnformeerd wanneer de gegevens zijn vastgelegd of verstrekt op grond van een wettelijke plicht.^{86 87}

5.2.1.4 Rechten van betrokkene

In de vorige sub paragraaf zijn de plichten van de verantwoordelijke besproken. In deze sub paragraaf worden de rechten van de betrokkene omschreven. De betrokkene heeft ten aanzien van zijn persoonsgegevens het recht op inzage, het recht op correctie en het recht op verzet. Deze rechten zullen nu worden toegelicht.

Recht op inzage

Iedereen heeft het recht om met redelijke tussenpozen te vragen welke persoonsgegevens ten aanzien van hem worden verwerkt. Op het verzoek om inzage wordt binnen 4 weken schriftelijk geantwoord. Wanneer persoonsgegevens worden verwerkt bevat de schriftelijke mededeling een volledig overzicht in begrijpelijke vorm, een omschrijving van het doel of doeleinde van de verwerking, de categorie van gegevens waarop de verwerking betrekking heeft en de ontvangers of categorieën van ontvangers, alsmede beschikbare informatie over de herkomst van de gegevens. Voordat de verantwoordelijke een schriftelijke mededeling doet en een derde zou hier naar verwachting bedenkingen bij hebben dan wordt die derde in de gelegenheid gesteld om zijn zienswijze naar voren te brengen indien de mededeling gegevens bevat die de derde betreffen. Dit hoeft niet wanneer het onmogelijk blijkt of een onevenredige inspanning kost. Wanneer hierom gevraagd wordt doet de verantwoordelijke mededeling omtrent de logica die ten grondslag ligt aan de geautomatiseerde verwerking van hem betreffende gegevens.⁸⁸

⁸⁵ L.B. Sauerwein & J.J. Linneman, *Handleiding voor verwerkers van persoonsgegevens*, Den Haag: Ministerie van Justitie 2002, p. 35.

⁸⁶ L.B. Sauerwein & J.J. Linneman, *Handleiding voor verwerkers van persoonsgegevens*, Den Haag: Ministerie van Justitie 2002, p. 35.

⁸⁷ Art.33 jo. 34 Wbp.

⁸⁸ Art. 35 Wbp.

Recht op correctie

De betrokkene kan op grond van de Wbp de verantwoordelijke verzoeken de gegevens, zoals die bij het recht op inzage zijn gegeven, te verbeteren, aan te vullen, te verwijderen, of af te schermen wanneer deze feitelijk onjuist zijn, voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn of wanneer de gegevens in strijd met een wettelijk voorschrift worden verwerkt.⁸⁹ Wanneer de betrokkene het bovenstaande verzoekt, moet hij de aan te brengen wijzigingen in het verzoek meeleveren.

Wanneer de gegevens gecorrigeerd worden, moeten derden die deze gegevens ontvangen hebben op de hoogte worden gesteld van de wijziging. Hoe ingrijpender de aangebrachte correctie, hoe verder de onderzoeksplicht strekt. Er hoeft geen mededeling te worden gedaan aan derden wanneer het onmogelijk is om deze derden op te sporen of onevenredige inspanning zou moeten leveren om deze derden op te sporen. Om erachter te komen of er sprake is van een onevenredige inspanning, moeten de belangen van de verantwoordelijke worden afgewogen tegen de belangen van de betrokkene.^{90 91}

Als de verantwoordelijke de correctie weigert dan moet deze weigering met redenen zijn omkleed. Het kan in bepaalde gevallen ook zo zijn dat persoonsgegevens zijn vastgelegd op een gegevensdrager. Een gegevensdrager is een apparaat of voorwerp waar gegevens op kunnen worden geschreven en bewaard. Het gaat dan om bijvoorbeeld een harde schijf, geheugenkaart of een usb-stick. Wanneer gegevens zijn opgeslagen op een gegevensdrager waarin geen wijzigingen kunnen worden aangebracht, moet de verantwoordelijke voorzieningen treffen die nodig zijn om de gebruiker van de gegevens te informeren over de onmogelijkheid van verbetering, aanvulling, verwijdering of afscherming ondanks het feit dat er grond is voor aanpassing van de gegevens.⁹²

Recht op verzet

In de Wbp is geregeld dat betrokkene het recht hebben bij de verantwoordelijke te allen tijde verzet aan te tekenen wanneer er sprake is van persoonlijke omstandigheden.⁹³ De verantwoordelijke zal dan beoordelen of het verzet gerechtvaardigd is. Als dit het geval is, beëindigt de verantwoordelijke onmiddellijk de verwerking van de persoonsgegevens. Verder regelt de Wbp dat de betrokkene ook verzet mag aantekenen als zijn persoonsgegevens worden verwerkt voor directe marketing doeleinden.⁹⁴

5.2.2 Geneeskundige behandelovereenkomst

5.2.2.1 Achtergrond

‘In 1977 vroeg de regering aan de toenmalige Centrale Raad voor de Volksgezondheid om advies uit te brengen over de wettelijke vormgeving van de patiëntenrechten. Daartoe werd een commissie ingesteld onder voorzitterschap van professor Leenen. In de periode 1980-1982 publiceerde deze commissie een vijftal deeladviezen, die op de verschillende

⁸⁹ Art. 36 Wbp.

⁹⁰ L.B. Sauerwein & J.J. Linneman, *Handleiding voor verwerkers van persoonsgegevens*, Den Haag: Ministerie van Justitie 2002, p.37.

⁹¹ Artikel 38 Wbp.

⁹² Artikel 36 Wbp.

⁹³ Art. 40 Wbp.

⁹⁴ Art. 41 Wbp.

juridische relaties tussen hulpverleners en patiënten betrekking hadden. Aangezien het hele 'veld' van de gezondheidszorg in deze Raad en de voorbereidende commissie waren vertegenwoordigd, werd hiermee een grote overeenstemming over de patiëntenrechten uitgedrukt. Onderdeel van de aanbevelingen was een wettelijke regeling van een aantal patiëntenrechten. Daartoe werd vervolgens in een motie ook in de Tweede kamer gepleit. In 1987 bracht de regering een voorontwerp op de WGBO uit en in 1990 het definitieve wetsontwerp.⁹⁵ Deze regeling is opgenomen in boek 7 van het burgerlijk wetboek in titel 7 afdeling 5. De WGBO heeft specifieke regels ten aanzien van privacy, en de Wbp stelt de algemene regels. De Wbp en de WGBO vullen elkaar in dit opzicht aan.

De WGBO regelt naast het recht op privacy en de geheimhouding van medische gegevens ook het recht op informatie over de medische situatie, de toestemming voor een medische behandeling, inzage in het medisch dossier, het recht op een vrije artskeuze en de vertegenwoordiging van patiënten die niet zelf kunnen beslissen. Naast rechten regelt de regeling uit boek 7 ook plichten. Dit is de plicht dat de patiënt de zorgverlener goed, eerlijk en volledig op de hoogte moet stellen van zijn problematiek. De patiënt moet zo veel mogelijk meewerken en adviezen opvolgen. Verder regelt de regeling dat een arts in sommige gevallen zonder toestemming een medische ingreep mag doen.⁹⁶

De WGBO valt onder het privaatrecht en binnen dit privaatrecht wordt een onderscheid gemaakt in regelend en dwingend recht. Regelend recht houdt in dat het recht een richtlijn geeft aan hoe private partijen hun verhouding kunnen regelen. Als ze niets anders regelen geldt de wettelijke regeling maar hier kan dus van worden afgeweken. Bij dwingend recht kan dit niet. Wanneer partijen dan iets anders regelen heeft dit geen gelding. Bijna alle bepalingen van de WGBO zijn dwingend recht en hier kan dus niet van worden afgeweken.⁹⁷ De WGBO geeft dus een dwingend kader voor de overeenkomst tussen partijen met betrekking tot de geneeskundige behandeling van een patiënt.⁹⁸

Relevant voor dit onderzoek is het medische beroepsgeheim dat van toepassing is op grond van de WGBO.⁹⁹ Dit betekent dat de hulpverlener waar de WGBO van toepassing is niet zonder toestemming van de cliënt medische gegevens mag delen. Hier zijn wel een aantal uitzonderingen op, namelijk bij een wettelijke plicht, conflict van plichten of een zwaarwegend belang. Een conflict van plichten kan zich voordoen wanneer een zwaarwegend belang van de patiënt of een ander dan de patiënt de doorbreking van de geheimhoudingsplicht rechtvaardigt, omdat het bewaren van het geheim voor de patiënt of de ander ernstig nadeel of gevaar oplevert. Het moet dan gaan om een noodsituatie.¹⁰⁰

5.2.2.2 Reikwijdte WGBO

De WGBO spreekt niet specifiek over bepaalde beroepsbeoefenaren maar spreekt over hulpverlener. Buiten zorginstellingen zoals ziekenhuizen is het soms moeilijk te bepalen of er sprake is van verpleging en/of verzorging in het kader van een geneeskundige behandeling.

⁹⁵ E-B. Veen, *De WGBO. De betekenis voor de hulpverleners in de gezondheidszorg*, Den Haag: Sdu Uitgevers 2002, p. 3.

⁹⁶ www.dwangindezorg.nl → rechten → wetten → WGBO.

⁹⁷ Art. 7:486 BW.

⁹⁸ E-B. Veen, *De WGBO. De betekenis voor de hulpverleners in de gezondheidszorg*, Den Haag: Sdu Uitgevers 2002.

⁹⁹ Art. 7:457 jo. 7:454 BW.

¹⁰⁰ *Geheimhouding van medische gegevens* (informatieblad van het CBP), februari 2011.

Om de vraag te kunnen beantwoorden of de WGBO van toepassing is moeten er twee aspecten worden bekeken.

1. Welke overeenkomsten vallen binnen het bereik van de WGBO?
2. Wanneer hebben partijen zo'n overeenkomst gesloten? ¹⁰¹

In boek 7 BW staat dat wanneer een opdrachtgever zich verbindt tot het verrichten van handelingen op het gebied van de geneeskunst en deze handelingen rechtstreeks betrekking hebben op de patiënt er sprake is van een overeenkomst inzake geneeskundige behandeling. ¹⁰² De patiënt is degene op wiens persoon de handelingen rechtstreeks betrekking hebben. Het burgerlijk wetboek verstaat onder geneeskundige behandeling: ¹⁰³

a. alle verrichtingen - het onderzoeken en het geven van raad daaronder begrepen - rechtstreeks betrekking hebbende op een persoon en ertoe strekkende hem van een ziekte te genezen, hem voor het ontstaan van een ziekte te behoeden of zijn gezondheidstoestand te beoordelen, dan wel deze verloskundige bijstand te verlenen;

b. andere dan de onder a bedoelde handelingen, rechtstreeks betrekking hebbende op een persoon, die worden verricht door een arts of tandarts in die hoedanigheid.

Een hulpverlener in de zin van de WGBO is een instelling of een zelfstandig gevestigd beroepsbeoefenaar, maar niet de werknemer van een zondanige contractpartij. Het is in de praktijk wel de werknemer die namens zijn werkgever een behandelingsovereenkomst met de patiënt aan gaat. De verplichtingen uit de WGBO rusten daarmee op die werkgever. ¹⁰⁴

In de memorie van toelichting van de WGBO staat dat de regeling ook van toepassing is op overeenkomsten met een beperkt, zeer specifiek doel, ter uitvoering waarvan handelingen op het gebied van de geneeskunst moeten worden verricht en dat deze overeenkomsten dus ook overeenkomsten zijn in de zin van deze wet. ¹⁰⁵

Uit de memorie van toelichting van de WGBO blijkt dat zowel de handelingen op het gebied van de geneeskunst als de daarbij behorende "aanpalende" handelingen onder de reikwijdte van de wet vallen. ¹⁰⁶ Aanpalende handelingen zijn handelingen die een samenhangend geheel vormen met de handelingen op het gebied van de geneeskunst. Maatschappelijk werk en paramedische verrichtingen vallen volgens de memorie van toelichting niet onder de reikwijdte van de WGBO. ¹⁰⁷ Voor Traverse betekent dit dat de WGBO van toepassing op handelingen die onder de geneeskundige behandeling vallen, zoals het intramusculair toedienen van medicijnen, en alle handelingen die noodzakelijk samenhangen met deze behandeling. Het verdere begeleidingsproces dat niet noodzakelijk is voor de geneeskundige behandeling van de cliënt, daar is de Wbp van toepassing. De relevante handelingen van Traverse zijn het bepalen van bloedglucosewaarde, intramusculair injecteren, subcutaan injecteren, toedienen van insuline, het toedienen en verstrekken van medicatie.

¹⁰¹ E-B. Veen, *De WGBO. De betekenis voor de hulpverleners in de gezondheidszorg*, Den Haag: Sdu Uitgevers 2002.

¹⁰² Art. 7:446 BW.

¹⁰³ Art. 7:446 lid 2 BW.

¹⁰⁴ E-B. Veen, *De WGBO. De betekenis voor de hulpverleners in de gezondheidszorg*, Den Haag: Sdu Uitgevers 2002.

¹⁰⁵ *Kamerstukken II 1989/90*, 21 561, nr 3 (MvT).

¹⁰⁶ *Kamerstukken II 1989/90*, 21 561, nr 3 (MvT), p.9.

¹⁰⁷ *Kamerstukken II 1989/90*, 21 561, nr 3 (MvT), p.9.

5.3 Algemene Verordening Gegevensbescherming

De Europese privacy verordening die in de maak is vervangt in de nabije toekomst de nu geldende richtlijn 95/46/EG. Op de laatstgenoemde richtlijn is de Wbp gebaseerd. Deze nieuwe verordening zal bestaan uit een Algemene verordening gegevensbescherming (hierna AVG) en een richtlijn die betrekking heeft op de bescherming van persoonsgegevens die worden verwerkt in het kader van potentiële en justitiële activiteiten. Hierna wordt een schema weergegeven waarin de grootste veranderingen van de AVG ten opzichte van de nu geldende wetgeving zijn verwerkt.

Artikel AVG	Gebaseerd op	Opgenomen in de Wbp	Verandering
Art. 5	Art. 6 richtlijn 95/46/EG	Art.6, 7 en 8	- Transparantiebeginsel - Verduidelijking van het beginsel van minimale gegevensverwerking - Vaststelling van alomvattende verantwoordelijkheid en aansprakelijkheid van de voor de verwerking verantwoordelijke
Art.7			- Verantwoordelijke moet aan kunnen tonen dat er toestemming is voor de verwerking van zijn persoonsgegevens
Art.11	Ingegeven door de Resolutie van Madrid		- Transparant en eenvoudig toegankelijk privacybeleid waarin ook duidelijk de rechten van de betrokkene opgenomen zijn
Art. 14	Art. 11 en 12 richtlijn 95/46/EG		- Mededelingsplicht
Art. 17	Art. 12 onder b richtlijn 95/46/EG		- Betrokkene krijgt het recht om te worden vergeten en om gegevens te laten wissen
Art. 18			- Recht op gegevensoverdraagbaarheid
		Art.27	- Melden van een geheel of gedeeltelijke verwerking van persoonsgegevens
Art. 31	Art. 4 lid 3 Richtlijn 2002/58/EG		- Meldpunt voor datalekken
Art. 33			- Bij verwerkingen die bijzondere risico's inhouden wordt er een beoordeling uitgevoerd over het effect van de beoogde verwerkingen op de bescherming van persoonsgegevens.
Art. 35	Art.18 lid 2 richtlijn		- In bepaalde gevallen, waaronder bij een onderneming van ten

	95/46/EG		minste 250 medewerkers, moet een functionaris voor de gegevensbescherming worden aangesteld.
Art. 79			- Het CBP kan een administratieve sanctie opleggen van €1.000.000 of 2% van de jaarlijkse omzet.

Plichten voor Traverse

Uit de AVG komen de volgende plichten naar voren die van toepassing zijn op Traverse. Traverse moet transparant zijn in de informatie die zij verwerkt ten aanzien van de cliënt. Traverse moet kunnen aantonen dat er toestemming is gegeven door de cliënt voor het verwerken van persoonsgegevens, en dus niet alleen een toestemming voor het delen van gegevens met externen. Verder moet er een transparant privacybeleid worden opgesteld, die eenvoudig toegankelijk is en waarin de rechten van de betrokkene zijn meegenomen. Wanneer gegevens worden verzameld moet Traverse de betrokkene hiervan op de hoogte stellen en over een aantal zaken informeren zoals de identiteit van de verantwoordelijke. Het melden van geheel of gedeeltelijke verwerking van persoonsgegevens vervalt. Hiervoor was Traverse al uitgezonderd, dit heeft dus verder geen invloed. Er wordt wel een meldpunt voor datalekken in het leven geroepen. Dit is een verplichting om inbreuken in verband met persoonsgegevens te melden. Een andere verplichting die de AVG met zich meebrengt is dat er een beoordeling uitgevoerd moet worden over het effect van een beoogde verwerking van persoonsgegevens wanneer de verwerkingen gezien hun aard, reikwijdte of doeleinden bijzondere risico's inhouden voor de rechten en vrijheden van de betrokkenen. Er is sprake van een verwerking met een bijzonder risico bij een systematische en uitgebreide beoordeling van aspecten van de persoonlijkheid van een natuurlijke persoon bijvoorbeeld om met name zijn economische situatie, verblijfplaats, gezondheid, persoonlijke voorkeuren, betrouwbaarheid of gedrag te analyseren of te voorspellen, die is gebaseerd op geautomatiseerde verwerking en waarop maatregelen zijn gebaseerd waaraan voor die persoon rechtsgevolgen zijn verbonden of die hem in aanzienlijke mate treffen.¹⁰⁸

Bij een onderneming met meer dan 250 medewerkers is het verplicht om een functionaris voor gegevensbescherming aan te stellen. Dit geldt dus ook voor Traverse. Het is ook mogelijk om met een groep ondernemingen één functionaris aan te stellen.

Rechten cliënten

De cliënt krijgt met de AVG het recht om te worden vergeten. Dit houdt in dat de cliënt het recht heeft de verantwoordelijke te verzoeken zijn gegevens te wissen en te verzoeken dat de verdere verspreiding van gegevens achterwege blijft. Ook krijgt de cliënt het recht van gegevensoverdraagbaarheid. Dit betekent dat de cliënt het recht heeft om gegevens van het ene elektronische verwerkingssysteem naar het andere over te dragen.

College Bescherming Persoonsgegevens

Het CBP heeft de bevoegdheid gekregen om hogere administratieve sancties te geven. Zo kan het CBP een boete opleggen van €1.000.000 of 2% van de omzet bij een onderneming.

¹⁰⁸ COM(2012)11, art. 33.

5.4 Slot

De Wet bescherming persoonsgegevens is als uitvoering van de Europese richtlijn tot stand gekomen. De wet geeft voorwaarde voor de verwerking van persoonsgegevens en geeft plichten aan de verantwoordelijke en rechten aan de betrokkene. De WGBO is van toepassing op zowel handelingen op het gebied van de geneeskunst als de daarbij behorende “aanpalende” handelingen. Wanneer de AVG in werking treed zullen er een aantal veranderingen plaats vinden. Deze veranderingen hebben ook invloed op Traverse.

Hoofdstuk 6. Conclusies en aanbevelingen

Met dit onderzoek wordt antwoord te geven op de vraagstelling: “Welke aanbevelingen kunnen er worden gedaan over de bescherming van de privacy van cliënten van Traverse, met betrekking tot de toegang tot digitale cliëntdossiers en het delen van persoonsgegevens intern en in samenwerking/contact met derden, gelet op de wettelijke verplichtingen?” Voor het beantwoorden van deze vraag is gebruik gemaakt van deelvragen die in het onderzoek beantwoord zijn. Dit hoofdstuk is opgedeeld in twee paragrafen met ieder een aantal subparagrafen. De eerste paragraaf, 6.1, geeft de conclusies te beginnen subparagrafen over het digitaal cliëntdossier en vervolgens over het delen van gegevens van cliënten. Paragraaf 6.2 gaat over de aanbevelingen die gegeven zijn naar aanleiding van de conclusies. In de eerste subparagraaf, 6.1.1.1, wordt antwoord gegeven op de vraag of de autorisatie van de toegang tot de digitale dossiers rechtmatig is. In subparagraaf 6.1.1.2 wordt antwoord gegeven op de vraag of er sprake is van logging, of daar controle op is en of dit rechtmatig is. Logging is het bijhouden wie wanneer een dossier raadpleegt. In de subparagraaf daarna wordt antwoord gegeven op de vraag of de toegang tot het digitaal cliëntdossier voldoende beschermd is. In de paragrafen hierna wordt antwoord gegeven op de vraag of het delen van informatie van cliënten rechtmatig plaatsvindt binnen Traverse. De subparagraaf 6.1.2.1 beantwoordt of het delen van cliëntgegevens intern rechtmatige gebeurd. In paragraaf 6.1.2.2 wordt beantwoord of het delen van cliëntgegevens met externen rechtmatig gebeurd. De volgende paragraaf, 6.1.3, beantwoordt de vraag wat er veranderd voor Traverse met de komst van de Algemene Verordening Gegevensbescherming en paragraaf 6.1.4 beantwoordt in welke gevallen Traverse onder de WGBO valt en wanneer ze onder de Wbp valt. Vervolgens wordt in paragraaf 6.2 de aanbevelingen gegeven die gedaan zijn naar aanleiding van de getrokken conclusies. De aanbevelingen zijn verdeeld in subparagrafen met respectievelijk de onderwerpen: de toegang tot digitale cliëntdossier, het beveiligen van de toegang, het delen van cliëntgegevens, de Algemene Verordening Gegevensbescherming en de toepassing van de WGBO en de Wbp.

6.1 Conclusies

6.1.1 De toegang tot digitale cliëntdossiers

6.1.1.1 Autorisatie van de toegang tot het digitaal cliëntdossier

Uit het onderzoek is gebleken dat Traverse zich bij het verlenen van de autorisatie voor de toegang tot digitale cliëntdossiers niet houdt aan de wet. De Wbp geeft aan dat de toegang tot gegevens in gedigitaliseerde cliëntendossiers alleen rechtmatig is, indien en voor zover de medewerker rechtstreeks betrokken is bij de behandeling of zorgverlening van een cliënt. Of wanneer de medewerker betrokken is bij de beheersmatige afwikkeling van die behandeling/zorgverlening en de toegang beperkt blijft tot de gegevens die noodzakelijk zijn voor de uitvoering van hun taken.¹⁰⁹ Binnen Traverse wordt de autorisatie verleend op grond van de functie van de medewerker. Daarbij wordt een onderscheid gemaakt tussen medewerkers die betrokken zijn bij het beheer van de instelling en medewerkers die zijn betrokken bij de behandeling of begeleiding van cliënten. Uit het rapport van het CBP blijkt dat autorisatie op grond van functie geen juiste uitwerking is van wat de Wbp voorschrijft.

¹⁰⁹ Art. 21 lid 1 onder a Wbp.

Deze wijze van autoriseren is niet zodanig dat daarmee wordt bereikt dat uitsluitend toegang mogelijk is tot gegevens in cliëntendossiers voor medewerkers voor wie dat gelet op een rechtstreekse betrokkenheid bij de behandeling, verzorging of begeleiding van cliënten noodzakelijk is.¹¹⁰ Verder wordt door het CBP geconstateerd dat ook ten aanzien van administratief ondersteunende medewerkers wordt vereist dat zij slechts toegang krijgen tot gegevens van patiënten indien en voor zover noodzakelijk. Deze noodzaak bestaat alleen indien en voor zover cliënten tot hun werkcontext horen. Wanneer deze werkcontext niet wordt betrokken in de autorisatie van administratief ondersteunende medewerkers, is er sprake van autorisatie die niet voldoet aan de Wbp.^{111 112} Bovenstaande betekent voor Traverse bijvoorbeeld dat de medewerkers die aangesteld zijn als woonbegeleider niet onmiddellijk de autorisatie krijgen voor alle cliëntdossiers maar slechts voor diegene die ze ook daadwerkelijk begeleiden. Dit geldt ook voor de medewerkers die aangesteld zijn als Topper en op alle functies inzetbaar moeten zijn. Zij hebben nu alle rechten gekregen, maar ze zouden alleen de rechten mogen krijgen voor de toegang tot de dossiers van cliënten waarbij er sprake is van een rechtstreekse betrokkenheid.

6.1.1.2 Logging en controle

Uit het onderzoek is gebleken dat Traverse niet voldoet aan de vereisten uit de Wbp met betrekking tot de maatregelen die genomen moeten worden om de privacy van cliënten te beschermen. Halverwege de onderzoeksperiode is Traverse overgestapt van het cliëntregistratiesysteem Regas naar Regas Webbased. Dit heeft er toe geleid dat iedere medewerker een eigen inlognaam en wachtwoord heeft gekregen voor Regas Webbased. Het is daardoor mogelijk elke actie van elke medewerker te loggen en dit wordt ook gedaan. Hierdoor voldoet Traverse aan wat de Wbp voorschrijft wat betreft logging. De controle op deze logging is ook een vereiste uit de wet, en hier voldoet Traverse nog niet aan. Er hoort een periodieke controle plaats te vinden over de gelogde activiteiten. Traverse controleert slechts wanneer er vermoeden is van misbruik van de gegevens of wanneer er een klacht binnen komt. Zorginstellingen waarbij geen periodieke controle van alle logging plaatsvindt voldoen niet aan de Wbp.^{113 114}

6.1.1.3 Beveiliging toegang

Traverse handelt met betrekking tot het beschermen van de toegang tot het digitaal cliëntendossier in strijd met de Wbp.¹¹⁵ De toegang tot de digitale cliëntdossiers is bij Traverse beschermd met een individuele inlognaam en wachtwoord. Uit een gesprek met het CBP is gebleken dat wanneer er sprake is van medische gegevens in een digitaal dossier, deze dossiers extra beschermd dienen te zijn. Dit wil zeggen met een tweefactor authenticatie. Dit onderscheid is bij Traverse niet aanwezig. Elk dossier is enkel beveiligd met een inlognaam en wachtwoord en daarmee voldoen ze niet aan de wettelijke eisen met betrekking tot de bescherming van het digitaal cliëntdossier.

¹¹⁰ *Toegang tot digitale cliëntendossiers binnen zorginstellingen* (rapport van het CBP), Den Haag: juni 2013, p.12.

¹¹¹ Art.13 Wbp.

¹¹² *Toegang tot digitale cliëntendossiers binnen zorginstellingen* (rapport van het CBP), Den Haag: juni 2013, p.12-13.

¹¹³ Art.13 Wbp.

¹¹⁴ *Toegang tot digitale cliëntendossiers binnen zorginstellingen* (rapport van het CBP), Den Haag: juni 2013, p.17.

¹¹⁵ Art. 13 Wbp.

Het CBP geeft aan gebruik te maken van de Code voor Informatiebeveiliging en NEN 7510 bij de controle op de passende technische en organisatorische genomen maatregelen. Dit zijn beveiligstandaarden die het hele terrein van de informatiebeveiliging binnen een organisatie afdekken.

6.1.2 Delen van informatie

Het delen van informatie gebeurt zowel intern als extern. Intern gebeurt het zowel bewust als onbewust. In paragraaf 6.1.2.1 wordt ingegaan op het delen van de informatie intern en in paragraaf 6.1.2.2 wordt ingegaan op het informatie delen met externen.

6.1.2.1 Delen van informatie intern

Intern wordt de informatie van cliënten in strijd met de Wbp gedeeld. Uit verschillende interviews met medewerkers van Traverse is gebleken dat niet iedereen op de hoogte is van het beleid. Dit komt vooral omdat het beleid onduidelijk is vastgelegd en er geen specifieke regels zijn opgesteld voor het delen van gegevens intern. De meeste medewerkers blijken wel op de hoogte te zijn van de toestemming die nodig is van de cliënt bij het delen van gegevens, maar weten niet wanneer deze toestemming precies nodig is. Het delen van gegevens intern gebeurt zowel bewust als onbewust. Het onbewust delen van gegevens gebeurt op momenten dat cliënten telefonisch contact opnemen met de receptie. Tijdens deze gesprekken noemt de receptioniste vaak de naam en problematiek van de cliënt over wie het telefoongesprek gaat. De deur tussen de receptieruimte en een kantoorruimte staat regelmatig open. Hierdoor zijn de gesprekken hoorbaar in de gang en op diverse werkplekken. Een persoonsgegeven is volgens de Wbp elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.¹¹⁶ Door de gegevens die de receptioniste herhaalt is een natuurlijke persoon te identificeren. De persoonsgegevens worden in deze verwerkt door ze hoorbaar ter beschikking te stellen aan iedereen die zich binnen gehoorafstand bevindt zonder dat hiervoor een rechtmatige grondslag aanwezig is. Dit is in strijd met de Wbp.¹¹⁷

Daarnaast worden er volgens een teamleider op haar afdeling geregeld casussen besproken waarbij deuren worden opengelaten en informatie over cliënten hoorbaar is. Hiervoor geldt hetzelfde als hierboven geconcludeerd is, dit is in strijd met de Wbp.¹¹⁸

Het bewust delen van persoonsgegevens van cliënten intern gebeurt in overleg of per mail. Dit is toegestaan wanneer het wordt gedeeld tussen medewerkers die direct betrokken zijn bij de verzorging/ begeleiding van de cliënt en het delen van deze informatie noodzakelijk is. Voor de ondersteunende diensten geldt ook dat de informatie alleen gedeeld mag worden indien en voor zover noodzakelijk. Het ontbreken van beleid rondom het delen van informatie levert echter onzekerheid op over de rechtmatigheid van deze verwerking van persoonsgegevens. Via Regas wordt er controle uitgeoefend door middel van autorisaties op de toegang tot de gegevens. Op mail of overleg is deze controle er niet en door het ontbreken van beleid maakt dit de kans op onrechtmatige verwerking van persoonsgegevens groter. Het is nu niet duidelijk welke gegevens wel gedeeld mogen worden en welke niet. Ook uit eigen ervaring van de onderzoeker is gebleken dat al snel alle gegevens van de cliënt op tafel liggen. De afweging welke gegevens noodzakelijk zijn om te verstrekken wordt

¹¹⁶ Art. 1 onder a Wbp.

¹¹⁷ Art. 9 jo 13 Wbp.

¹¹⁸ Art. 9 jo 13 Wbp.

niet gemaakt. Wanneer er onnodige informatie gedeeld wordt, is dit ook in strijd met de Wbp.¹¹⁹

6.1.2.2 Delen van informatie extern

Extern worden de gegevens niet in strijd met de wet gedeeld. Dit komt omdat het beleid duidelijker is voor medewerkers en er met politie, justitie en een jurist gespecialiseerd in Privacyrecht wordt gezocht naar een juridisch kader om efficiënt gegevens te delen in samenwerkingsverband. Uit interviews is naar voren gekomen dat men, vergeleken met het intern delen van informatie, beter op de hoogte is wanneer medewerkers persoonsgegevens van cliënten mogen delen met externen. Men is op de hoogte dat bij intake een formulier is ondertekend door de cliënt voor toestemming om zijn gegevens te delen met bepaalde instanties. Een aantal medewerkers gaf zelfs aan nogmaals contact op te nemen met de cliënt als er overleg plaats zou vinden met de huisarts of GGZ, ook al was de toestemming al gegeven via het ondertekende formulier. Men is op de hoogte dat alleen die gegevens mogen worden verstrekt die een doel dienen. En dan heeft men het over het doel van een goede begeleiding van de cliënt.

Het toestemmingsformulier dat getekend wordt door de cliënt bij intake, geldt voor het gehele traject van de cliënt. Dit is een geldige toestemming in de zin van de Wbp. Dit is bevestigd in een gesprek met het CBP. Wel is opgemerkt door het CBP dat zodra er gegevens wijzigen, de toestemming opnieuw moet worden gevraagd.

Binnen het Zorg-en Veiligheidshuis is men bezig met het maken van goede afspraken en een juridisch kader met betrekking tot het delen van gegevens in samenwerkingsverband.

Binnen Housing First geldt hiervoor hetzelfde. De verschillende instellingen werken samen om gezamenlijk de cliënt een goede begeleiding te kunnen bieden. Binnen de overleggen die gevoerd worden zullen persoonsgegevens worden gedeeld, dit zal gaan over de cliënten die gezamenlijk worden begeleid en hierbij is een directe betrokkenheid en noodzakelijkheid aanwezig voor een goede begeleiding. Er wordt binnen dit samenwerkingsverband gekeken naar de afspraken die gemaakt zijn bij het Zorg- en Veiligheidshuis en naar de richtlijnen die gemaakt zijn voor bemoeizorg.

6.1.3 Algemene Verordening Gegevensverwerking

Met de Algemene Verordening Gegevensverwerking (Hierna AVG) in aantocht zullen er een aantal dingen veranderen. De inhoud van de verordening staat nog niet vast maar er wordt uitgegaan van de versie zoals hij nu is. Hierna volgt een bespreking van de veranderingen die plaats zullen vinden.

- De AVG legt op dat iedere instelling met meer dan 250 werknemers verplicht is om een functionaris voor de gegevensbescherming aan te stellen.¹²⁰ Traverse heeft ongeveer 275 medewerkers en daarmee valt zij dus onder de verplichting om een functionaris aan te stellen.
- Er moet een transparant en eenvoudig toegankelijk privacybeleid worden opgesteld waarin ook de rechten van de betrokkenen zijn opgenomen.¹²¹ Een privacybeleid

¹¹⁹ Art. 21 lid 1 onder a Wbp.

¹²⁰ COM(2012)11, Art. 35.

¹²¹ COM(2012)11, Art. 11.

heeft Traverse al en hierin zijn ook de rechten van de betrokken opgenomen. Wel zal duidelijker moeten worden omschreven wat de voorwaarde zijn voor het verwerken van persoonsgegevens en dat deze voorwaarde ook gelden voor het intern delen van persoonsgegevens. De betrokkene krijgt met de AVG ook een nieuw recht, namelijk het recht tot rectificatie en uitwissing van zijn gegevens.¹²² Dit zal in het beleid van Traverse opgenomen moeten worden.

- De cliënten krijgen het recht om gegevens van het ene elektronische verwerkingssysteem naar het andere over te dragen.
- Verder moet Traverse op grond van de AVG kunnen aantonen dat ze toestemming hebben van de betrokkene voor de verwerking van zijn gegevens.¹²³ Aan dit vereiste voldoet Traverse door het toestemmingsformulier dat ondertekend wordt bij intake.
- De administratieve sanctie die het CBP op kan leggen wordt verhoogd tot €1.000.000 of 2% van de jaarlijkse omzet. In welke gevallen het CBP deze sancties op kan leggen is opgenomen in de AVG.¹²⁴ De onrechtmatigheden die zijn beschreven in paragraaf 6.1.1 vallen onder dit artikel en traverse dient deze punten dan ook te verbeteren zodat het geen boete kan krijgen wanneer de AVG in werking treedt.
- De AVG regelt dat er een meldpunt moet komen voor datalekken. Dit betekent voor Traverse dat de verantwoordelijke, door Traverse aangewezen de managers, een inbreuk in verband met een persoonsgegeven onverwijld, binnen 24 uur, moet melden bij het CBP.¹²⁵
- Daarnaast moeten gevoelige verwerkingsactiviteiten aan een privacyeffectenbeoordeling worden onderworpen.¹²⁶ Traverse valt op grond van de AVG onder de gevoelige verwerkingsactiviteiten.¹²⁷ Dit betekent dat de voor de verwerking verantwoordelijke of de verwerker die ten behoeve van de voor de verwerking verantwoordelijke optreedt een beoordeling uitvoert van het effect van de beoogde verwerking op de bescherming van persoonsgegevens.

6.1.3 Wbp en WGBO

Traverse heeft in een aantal gevallen te maken met processen in het kader van medische zorg. Voor Traverse betekent dit dat de WGBO van toepassing op handelingen die onder de geneeskundige behandeling vallen, zoals het intramusculair toedienen van medicijnen, en alle handelingen die noodzakelijk samenhangen met deze behandeling. Het verdere begeleidingsproces dat niet noodzakelijk is voor de geneeskundige behandeling van de cliënt, daar is de Wbp van toepassing. De relevante handelingen van Traverse zijn het bepalen van bloedglucosewaarde, intramusculair injecteren, subcutaan injecteren, toedienen van insuline, het toedienen en verstrekken van medicatie. Het gevolg van het van toepassing zijn van de WGBO is dat op die processen het beroepsgeheim rust. Dit betekent dat de

¹²² COM(2012)11, Art. 16 en 17.

¹²³ COM(2012)11, Art. 7.

¹²⁴ COM(2012)11, Art. 79.

¹²⁵ COM(2012)11, Art. 31.

¹²⁶ COM(2012)11, Art. 33.

¹²⁷ COM(2012)11, Art. 33 lid 2 onder a.

hulpverlener waar de WGBO van toepassing is niet zonder toestemming van de cliënt medische gegevens mag delen.

6.1.4 Slot

De aanbevelingen die volgen in de volgende paragraaf laten zien in hoeverre er antwoord is gegeven op de centrale vraag. De centrale vraag luidt:

“Welke aanbevelingen kunnen er worden gedaan over de bescherming van de privacy van cliënten van Traverse, met betrekking tot de toegang tot digitale cliëntdossiers en het delen van persoonsgegevens intern en in samenwerking/contact met derden, gelet op de wettelijke verplichtingen?”

De conclusies die in de bovenstaande paragraaf zijn getrokken maken duidelijk dat onderzoek is verricht naar de beschermingsgraad van de informatie van cliënten in digitale dossiers en van het delen van de informatie uit deze dossiers. Men blijkt in beide gevallen niet volledig te voldoen aan de regels gesteld in de Wbp om de privacy van cliënten voldoende te beschermen. In de volgende paragraaf volgen de aanbevelingen als bedoeld in de centrale vraag.

6.2 Aanbevelingen

6.2.1 toegang tot digitale cliëntdossiers

Er wordt aanbevolen om in het kader van autorisatie, beleid op te stellen waarin opgenomen wordt onder welke voorwaarde aan welke medewerker autorisatie kan worden verleend. De autorisatie overlaten aan het rechtsgevoel van de medewerkers van de afdeling automatisering leidt tot inbreuk op de bescherming van persoonsgegevens. In dit voorgestelde beleid moet worden verwerkt dat de autorisatie niet plaats vindt op functie maar op directe betrokkenheid of betrokken zijn bij de beheersmatige afwikkeling. Bij het opstellen van het beleid kan gebruik gemaakt worden van de Code voor Informatiebeveiliging en NEN 7510. Dit zijn beveiligstandaarden die het hele terrein van de informatiebeveiliging binnen een organisatie afdekken. Wanneer men aan deze standaarden voldoet, voldoet men ook aan de plicht uit het Wbp om technische en organisatorische maatregelen op te leggen.¹²⁸

6.2.2 Beveiliging toegang

Om de toegang tot de digitale cliëntdossiers waarin medische gegevens opgenomen zijn voldoende te beschermen, dient er extra bescherming van de gegevens plaats te vinden. Dit kan onder andere met een tweefactor authenticatie. Er wordt aanbevolen om een tweefactor authenticatie in gebruik te nemen voor het beschermen van de dossiers met medische gegevens.

6.2.3 Delen van gegevens

Er wordt aanbevolen om een beleid op te stellen waarin is opgenomen hoe men intern met persoonsgegevens van cliënten moet omgaan. In de cultuur van het bedrijf wordt te gemakkelijk over de cliënten gepraat. Er worden gezichten gehangen aan namen, er wordt doorgevraagd naar namen wanneer er slechts gesproken wordt over ‘cliënt’, puur uit nieuwsgierigheid en niet uit noodzakelijkheid en er wordt niet aan het afsluiten van ruimten gedacht wanneer daar over cliënten gesproken wordt. Ook een voorlichting aan

¹²⁸ Art. 13 Wbp.

medewerkers over de bescherming van persoonsgegevens is een aanbeveling, omdat dit de bewustwording vergroot over hoe belangrijk het beschermen van de gegevens is.

6.2.4 Algemene Verordening Gegevensbescherming

Wanneer de AVG in werking treedt moet er een functionaris voor de gegevensbescherming aangesteld worden. Dit kan Traverse doen door met een aantal instellingen één functionaris aan te stellen of alleen voor de eigen organisatie.

Er wordt daarnaast aanbevolen om het privacybeleid zo aan te passen dat zij voldoet aan de AVG. Dit houdt in ieder geval in dat het recht op rectificatie en uitwissing van de gegevens opgenomen moet worden in het privacybeleid. Dat het beleid transparant is en eenvoudig te toegankelijk. Verder moet worden opgenomen dat de cliënt het recht heeft van gegevensoverdraagbaarheid.

6.2.4 Wbp en WGBO

Er wordt aanbevolen om vast te leggen in welke gevallen voor Traverse de WGBO van toepassing is en welke bijkomstigheden daarbij komen kijken zodat de medewerkers weten welke regels van toepassing zijn. Er moet dan onder andere duidelijk worden gemaakt dat voor de processen waar de WGBO van toepassing is een medisch beroepsgeheim geldt. Aangeraden wordt om hier verder juridisch onderzoek naar te laten doen.

Literatuurlijst

Boeken

Bovend'Eert 2009

P.P.T. Bovend'Eert e.a., Grondwet voor het Koninkrijk der Nederlanden. Tekst en commentaar, Deventer: Kluwer 2009.

Koelewijn 2009

W.I. Koelewijn, Privacy en politiegegevens. Over geautomatiseerde normatieve informatieuitwisseling, Leiden: Leiden University Press 2009, p.56-57.

Leenen 2012

H.J.J. Leenen, J.K.M. Gevers & J. Legemaate, Handboek gezondheidsrecht. Deel 1. Rechten van mensen in de gezondheidszorg, Den Haag: Boom Juridische uitgevers 2012, p. 252.

Nollkaemper 2011

A. Nollkaemper, Kern van het internationaal publiekrecht, Den Haag: Boom Juridische uitgevers 2011, p. 488-489.

Veen 2002

E-B. Veen, De WGBO. De betekenis voor de hulpverleners in de gezondheidszorg, Den Haag: Sdu Uitgevers 2002.

Losse uitgaven

CBP 2012

Informatie delen in samenwerkingsverband (informatieblad van het CBP), februari 2012.

CBP 2013

Toegang tot digitale cliëntendossiers binnen zorginstellingen (rapport van het CBP), Den Haag: juni 2013.

CBP 2011

Geheimhouding van medische gegevens(informatieblad van het CBP), februari 2011.

Hustinx 1999

P.J. Hustinx, Nederland moet Europese privacyrichtlijn volgen (artikel gepubliceerd op cbp.nl), augustus 1999.

Sauerwein & J.J. Linneman 2002

L.B. Sauerwein & J.J. Linneman, Handleiding voor verwerkers van persoonsgegevens ,Den Haag: Ministerie van Justitie 2002

Elektronische bronnen

<eerstekamer.nl>

<tilburg.veiligheidshuis.org >

<smo-traverse .nl>

<CBPweb.nl>

< dwangindezorg.nl>

Bijlagen

- 1) Privacyreglement Traverse
- 2) Protocol bescherming persoonsgegevens Traverse
- 3) Schema rechtmatige verwerking Ministerie van Justitie
- 4) Werkinstructie aanmelding en intake Traverse
- 5) Werkinstructie cliëntdossier Traverse