Toets of de WBP binnen Vitalis wel vitaal is?

Een onderzoek naar de mate waarin de Wet Bescherming Persoonsgegevens wordt nageleefd binnen De Vitalis Zorg Groep.

The good news about privacy is that 84% of us are concerned about privacy.
The bad news is that we do not know what we mean.
(A.W. Branscomb, 1994).

ir. ing. Stephan J.T. van der Pol
S862614

Afstudeeronderzoek,
Afstudeerrichting Recht en Informatisering,
Faculteit der Rechtswetenschappen,
Universiteit van Tilburg.

April 2005.

1 Woord vooraf

Een uit de hand gelopen grap.....

Toen ik in 2001 aan de avondstudie Nederlands Recht begon, was “grap” de reden. Dit vraagt enige uitleg, want wie begint er nou bij wijze van grap aan een academische studie?
De oorzaak voor het starten aan de (toen nog) KUB was het feit dat tijdens mijn vorige studie de afstudeerfase was aangebroken en er geen college’s meer waren. Als antwoord op de sarcastisch bedoelde vraag “wat doen we nu met al die vrije avonden” kwam dus als serieus antwoord “we gaan colleges volgen in Tilburg”.

Na korte tijd bleek dat zowel de materie als de studenten dermate interessant waren, dat voorzetting een bewuste keuze werd.
De materie lag me goed; de diversiteit aan vakken, de inzichten die ontstonden met betrekking tot het recht in het dagelijks leven, de discussies over de grijze gebieden tussen goed of slecht danwel waar of onwaar, nieuwe theoretische kennis en vaardigheden, kortom een heel scala aan nieuwe uitdagingen motiveerden mij om meerdere avonden per week in een piepklein collegebankje plaats te nemen.
De studenten lagen me goed; de motivatie, de betrokkenheid, de behulpzaamheid die ertoe bijdroegen om meerdere malen per week in een piepklein collegebankje plaats te nemen (Wietske, heel erg bedankt voor de prettige samenwerking).
De docenten lagen me goed; vakkennis, afwisseling en humor zorgden ervoor dat ik meerdere malen per week....u kent het nu wel.....

Was alles koek en ei? Uiteraard niet; deadlines moesten gehaald worden, door de meer dan gemiddelde snelheid waarmee de vakken werden gevolgd, was ook de tentamenbelasting groot en schrijfopdrachten stapelden zich soms op. Maar alles verliep voorspoedig en na de rustperiode die op de tentamens volgde was ik telkens weer blij dat ik meerdere malen....inderdaad.....

En toen was het medio 2004 en was de lijst met te volgen vakken behoorlijk uitgedund en werd het tijd om serieus over afstuderen te gaan nadenken. Gelukkig dachten er mensen met mij mee wat resulteerde in deze opdracht; een opdracht op het raakvlak van theorie en praktijk met hierin het spanningsveld tussen dogmatiek en toepassing.

Inmiddels zit ik, slechts een paar maanden later dan de oorspronkelijke bedoeling was, de laatste teksten te schrijven en moet ik constateren dat ik me onbehaaglijk begin te voelen dat ik niet meer meerdere malen.....dat ja....

Met alleen nog de verdediging in de toekomst, zijn de mensen die ertoe hebben bijgedragen dat dit onderzoek en het bijbehorende verslag tot stand kwamen ook bijna van me af, maar niet zonder een woord van dank aan eenieder. Een woord van dank vooral voor Frank Budde voor de oorspronkelijke opdracht, voor Sjaak Nouwt voor de begeleiding welke een prima mix van vrijheid en sturing was en voor mijn eigen afdeling, de afdeling ICT van De Vitalis Zorg Groep, voor zowel de bijdragen aan de inhoud als ook voor de begeleiding bij het onder de knie krijgen van de techniek.
Ook de Raad van Bestuur en de directieraad van Vitalis hebben een grote rol gespeeld gedurende dit onderzoek en mogen niet onvermeld blijven, met name Nico van Dongen die zichzelf en een van zijn locaties in het diepe gooide tijdens de proefafnames van de interviews.

Graag draag ik dit onderzoek op aan mijn moeder, die de grootste motivator was om deze studie af te ronden. Op haar enige voorbehoud “jongen, jongen, als je maar geen advocaat wordt” blijf ik echter antwoorden.....”wie weet...”.

Stephan van der Pol,
Eindhoven, 8 april 2005.

Inhoudsopgave

2 Samenvatting

Op De Vitalis Zorg Groep rust, net zoals op alle andere verwerkers van persoonsgegevens, de plicht deze verwerkingen zorgvuldig en in overeenstemming met de wet te laten plaatsvinden. Om op een verantwoorde manier aan deze verplichting te voldoen is het noodzakelijk dat er een duidelijk overzicht is van zowel de gevoerde verwerkingen als ook van de concrete eisen die aan de diverse verwerkingen worden gesteld.

Om de gevoerde verwerkingen in kaart te brengen is een inventarisatie uitgevoerd, vergelijkbaar met de meldingsprocedure zoals deze door het CBP wordt voorgeschreven. Gebaseerd op een theoretische analyse van de begrippen die noodzakelijk zijn voor een volledige melding van verwerkingen, is een enquête ontwikkeld waarmee de relevante verwerkingen van De Vitalis Zorg Groep kunnen worden beschreven.

Na de inventarisatie is, uitgaande van het wettelijk kader voor bescherming van de informationele privacy, een grote hoeveelheid criteria afgeleid uit de literatuur. Deze criteria zijn verdeeld volgens de privacybeginselen transparantie, doelbinding, rechtmatige grondslag, kwaliteit, beveiliging en bewaartermijnen. De oorspronkelijke bedoeling was om elke beschreven verwerking te toetsen aan alle criteria om op deze manier tot een uitspraak per verwerking te komen of deze wel of niet aan de wettelijke eisen voldeed. De praktische omstandigheden van dit onderzoek noodzaakten echter tot een iets andere aanpak. Niet de verwerkingen zijn getoetst, maar de organisatie heeft, middels een quick-scan en detailinterviews, van zichzelf aangegeven in hoeverre wordt voldaan aan de privacybeginselen en dus aan de WBP.

De resultaten van deze interviews en enquêtes geven aanleiding tot de conclusie dat het met de vitaliteit van de WBP bij Vitalis niet goed is gesteld, met als voorbehoud dat de respons van dien aard is dat niet voor alle getoetste indicatoren statistisch relevante conclusies kunnen worden getrokken. Gezien de gebleken onbekendheid met de WBP zal de organisatie in de nabije toekomst veel aandacht moeten besteden aan bewustwording en beleid op dit gebied, waarbij een aantal concrete acties al in gang is gezet.

Voor wat betreft het werken met de WBP zijn er vanuit de dogmatiek en de juridische theorie argumenten aan te voeren waarom deze wet in de huidige vorm anders en beter kan. Vanuit de praktijk echter is de WBP wel degelijk een bruikbaar instrument; het geeft weliswaar niet direct antwoord op alle vragen, maar voor een organisatie die niet dagelijks met deze materie werkt biedt de wet een praktisch startpunt en werkt als een prima vuurtoren waarmee verantwoordelijken en betrokkenen op koers kunnen blijven bij het zoeken naar antwoorden op vraagstukken over informationele privacy.

3 Inleiding

3.1 Context

De Vitalis Zorg Groep dient zich, zoals alle organisaties die persoonlijke gegevens beheren en/of verwerken, te houden aan de WBP[1] en andere privacyregels. Voor delen van de organisatie of bepaalde functies kunnen nog additionele regels, voortvloeiend uit gedragscodes voor beroepsgroepen, van toepassing zijn.

De WBP is sinds 1 september 2001 van kracht, met een overgangstermijn van één jaar. Deze wet geeft aan wat de rechten zijn van iemand van wie gegevens worden gebruikt en wat de verplichtingen zijn van de instanties of bedrijven die gegevens gebruiken. Verzamelen en verwerken van persoonsgegevens dient te geschieden onder de voorwaarden en verplichtingen, zoals gesteld in de WBP. Dit heeft betrekking op het in kaart brengen van de verwerkingen en de doelen (moeten in overeenkomst zijn met elkaar), de waarborgen om onnodige verzameling of onjuist gebruik van gegevens te voorkomen (bewaartermijnen, beveiliging etc). Daarnaast moet een klacht- en inzagerecht gewaarborgd zijn.
De Vitalis Zorg Groep beschikt over een Functionaris Gegevensbescherming. Gegevensverwerkingen worden bij hem aangemeld in plaats van het CBP. De Vitalis Zorg Groep heeft haar beleidskader vastgelegd in de documenten: “Bescherming Persoonsgegevens” en “Functionaris voor de gegevensbescherming”.

Vanuit de bestaande wet- en regelgeving, maar ook vanuit kwaliteitsoogpunt binnen de eigen organisatie, is het noodzakelijk dat De Vitalis Zorg Groep aan de gestelde eisen voldoet.

3.2 Doelstelling

Inventariseren welke regelingen van toepassing zijn op de gegevensverzamelingen van De Vitalis Zorg Groep en wat de uit te voeren acties zijn om enerzijds de huidige stand van zaken vast te stellen en anderzijds benodigde acties m.b.t. de ICT te definiëren.

Meer specifiek zal dan binnen De Vitalis Zorg Groep een inventarisatie plaats dienen te vinden van de gegevensverwerkingen, die aangemeld worden bij de Functionaris Gegevensbescherming. Vervolgens zullen zonodig aanbevelingen gedaan worden, vanuit het perspectief van de WBP en de hieraan gerelateerde regelgeving. In het kader van dit project zullen aanbevelingen zich beperken tot de afdeling ICT. Voor het bovenstaande dient een “scan” ontwikkeld te worden waarmee de eigenschappen van de huidige verwerkingen eenduidig in kaart gebracht kunnen worden en door herhaalde toepassing actueel gehouden kunnen worden.

Binnen de Vitalis Zorg Groep zal zowel voor de diverse locaties als ook voor de ondersteunende diensten waaronder de ICT-afdeling een inventarisatie met eventuele aanbevelingen beschikbaar zijn, waarbij de aanbevelingen zich binnen dit onderzoek zullen beperken tot de afdeling ICT.

3.3 Probleemstellingen

Hoe krijgt de WBP zijn beslag binnen De Vitalis Zorg Groep en in hoeverre voldoen de bestaande verwerkingen aan de voorwaarden die door deze wet worden gesteld?
Welke acties moeten worden ondernomen om ervoor te zorgen dat het ICT-netwerk voldoet aan de eisen die door deze regelingen worden gesteld?

3.4 Onderzoeksdeelvragen

1. Welke gegevensverzamelingen zijn in gebruik bij De Vitalis Zorg Groep?
2. Welke zijn de relevante formele regelingen (wet)?
3. Welke zijn de relevante branche en/of gedragsregels?
4. Welke zijn de beleidsuitgangspunten en de ambitieniveaus van De Vitalis Zorg Groep?
5. Hoe kunnen bovenstaande regels worden omgezet in meetbare indicatoren?

[1] Wet van 6 juli 2000, Stb. 302, houdende regels inzake de bescherming van persoonsgegevens.

6. Hoe kunnen deze indicatoren worden omgezet in een Intranet-enquete?
7. Hoe dienen de uitkomsten te worden geanalyseerd c.q. gemeten?

3.5 Onderzoeksopzet

- Stap 1: op basis van de definities uit o.m. art 1 WBP inventariseren welke gegevensverzamelingen binnen De Vitalis Zorg Groep aanwezig zijn (beantwoorden deelvraag 1).

- Stap 2: beschrijven welke wettelijke voorwaarden uit WBP of andere regelingen (WGBO, sociaal recht, fiscaal recht etc) van toepassing zijn op de omgang met deze verzamelingen (zoals bewaartermijn, toegang, beveiliging etc.) (beantwoorden deelvraag 2,3 en 4).

- Stap 3: ontwikkelen en inzetten van een instrument om de huidige situatie voor wat betreft omgang met de in stap 1 gevonden verzamelingen in kaart te brengen (beantwoorden deelvraag 5 en 6) zodat de “IST-situatie” in kaart gebracht is.

- Stap 4: vergelijken van de “SOLL-situatie” uit stap 2 en de “IST-situatie” uit stap 3 om te komen tot actiepunten en aanbevelingen (beantwoorden deelvraag 7).

3.6 Leeswijzer

Dit verslag volgt qua indeling in grote lijnen de volgorde van de stappen uit de onderzoeksopzet. Het eerstvolgende hoofdstuk, hoofdstuk 4, biedt de lezer een kennismaking met De Vitalis Zorg Groep als zorginstelling en laat de noodzaak voor verwerking van persoonsgegevens zien.
Hoofdstuk 5 beschrijft de theoretische grondslagen voor de aan te melden en te beschrijven verwerkingen. Omdat voor de indeling van dit verslag de volgorde van de onderzoeksstappen richtinggevend is, wordt er afgeweken van het standaard onderscheid in materiele en formele bepalingen uit de WBP en worden in hoofdstuk 5 slechts begrippen beschreven die relevant zijn voor melding van verwerkingen.
Hoofdstuk 6 bevat de vertaling van wettelijke criteria voor toegestane verwerking uit de WBP naar praktische toetsingsvragen; ook hier is geen onderscheid gemaakt tussen formele en materiele criteria. Hiermee kunnen de in het vorige hoofdstuk verzamelde meldingen worden getoetst op het al of niet voldoen aan de WBP.
Hoofdstuk 7 is van belang omdat hierin de overstap wordt gemaakt van de theoretische kaders naar de praktijk van het onderzoek. Alle verzamelde criteria uit hoofdstuk 6 worden vertaald in concrete vragen die aan de organisatie gesteld kunnen worden.
In hoofdstuk 8 wordt kort aangegeven welke ervaringen zijn opgedaan bij de uitvoering van het onderzoek en worden de bijsturingen c.q. veranderingen ten opzichte van de oorspronkelijke uitgangspunten beschreven en verantwoord.
Hoofdstuk 9 geeft een kort overzicht van de belangrijkste statistische analyses die zijn uitgevoerd op de onderzoeksdata en toetst de waarde van de uitkomsten.
Het afsluitende hoofdstuk, hoofdstuk 10, beschrijft in het eerste deel de conclusies die uit dit praktische onderzoek kunnen worden getrokken, zowel op het hogere abstractieniveau van de WBP zelf als ook op basis van de ervaringen uit het onderzoek, kwalitatief en kwantitatief. In het tweede deel van hoofdstuk 10 zullen een aantal aanbevelingen aan de organisatie worden gedaan, zowel aanbevelingen ter beantwoording van de onderzoeksvragen maar ook algemene aanbevelingen ten aanzien van de omgang met de WBP.

4 Onderzoeksgebied: De Vitalis Zorg Groep

De totale organisatie is opgedeeld in drie werkmaatschappijen, waarbij de stichting De Vitalis Zorg Groep eigenaar is van verpleeghuis De Weerde en de exploitatie verzorgt van het verpleeghuis en de woonzorgcentra. Alle medewerkers hebben met deze stichting de arbeidsovereenkomst. De andere twee rechtspersonen[2] zijn eigenaar van de gebouwen, terreinen, de studio's en de (luxe) woonzorgappartementen. Deze drie rechtspersonen kennen een gezamenlijke Raad van Bestuur en Raad van Toezicht.

De Vitalis Zorg Groep heeft in totaal twintig vestigingen. In Eindhoven achttien, één in Helmond en één in Heerlen. Bij De Vitalis Zorg Groep werken momenteel 1390 medewerkers op circa 870 formatieplaatsen. Verder kan een beroep gedaan worden op 365 vrijwilligers. De stichting beschikt over 1866 verhuureenheden en 627 woonzorgappartementen. De Vitalis Zorg Groep huisvest circa 3000 senioren, een aantal dat zal stijgen tot meer dan 3600 bewoners in de toekomst. Aldus ressorteren onder de Vitalis Zorg Groep een aantal complexen welke bestaan uit een of meerdere locaties. In principe beschikt ieder complex over woonvoorzieningen in de sociale sector en het luxe segment, levert zowel AWBZ als particuliere zorg en behandeling evenals welzijnsfuncties en andere vormen van dienstverlening. Een en ander is uiteraard afhankelijk van de wensen en behoeften van (individuele) cliënten en andere gebruikers van de welzijnsfuncties en dienstverlening, bijvoorbeeld ouderen woonachtig in 'de wijk'.

De Vitalis Zorg Groep als geheel biedt vele vormen van woonvoorzieningen, zorg en dienstverlening. Zij onderscheidt zich van andere, soortgelijke organisaties door:
- het exploiteren van residentiele voorzieningen in zowel de sociale sector als het luxe segment;
- het aanbieden en beheren van de functies wonen, welzijn, zorg en behandeling in een samenhangend pakket;
- het aanbieden en beheren van voornoemde functies binnen één organisatorisch verband en binnen één gebouwencomplex (onder één dak)
- het herinvesteren van positieve resultaten uit vastgoed in de zorg.

Uitgaan van de wensen en behoeften van de klanten is niet alleen het vertrekpunt bij het exploiteren van de woonvoorzieningen en het bieden van samenhangende arrangementen op het gebied van wonen, zorg en welzijn maar nadrukkelijk ook bij het aansturen van de bedrijfsprocessen binnen de organisatie. De Vitalis Zorg Groep hanteert kwaliteit als managementprincipe, als middel om organisatiedoelen te bereiken. Het adagium is 'de goede dingen goed doen'. Dat impliceert beleidskeuzes maken op basis van de wensen en behoeften van (toekomstige) klanten en dat betekent continu verbeteren van zorg- en dienstverlening en borgen van gerealiseerde verbeteringen.

Het vertrekpunt van de beleidscyclus van De Vitalis Zorg Groep is, zoals in vele beleidscycli, een missie. In een missie, welke veelal tijdloze gegevens bevat, wordt de bestaansreden voor een organisatie beschreven. De geactualiseerde missie van De Vitalis Zorg Groep luidt als volgt:

Wij zijn een organisatie die aan cliënten een grote variatie woonvoorzieningen aanbiedt met een op hun behoefte, belevingen en verwachtingen afgestemd pakket aan verzorging, verpleging en overige diensten. Wij streven ernaar dat onze voorzieningen bijdragen aan een optimale kwaliteit van leven van de cliënt. Ons antwoord op een verzoek van een cliënt luidt in beginsel: 'Ja'. Wij zijn er op uit, dat onze dienstverlening door de cliënt als 'topkwaliteit' ervaren wordt[3]*.*

De dienstverlening waarvan sprake is in de missie van De Vitalis Zorg Groep vraagt overeenkomsten tussen bewoner en organisatie met betrekking tot wonen, verzorging, verpleging en andere diensten die door de bewoners worden gevraagd en door Vitalis worden aangeboden. Het sluiten en nakomen van deze overeenkomsten vraagt vastlegging en verwerking van grote hoeveelheden gegevens, niet alleen met betrekking tot de overeenkomst zelf maar ook over de (interne) processen die de nakoming mogelijk maken en welke, volgens de uitgangspunten van Vitais, continu op kwaliteit worden

[2] R.K. Stichting Bejaardenhuisvesting Eindhoven en stichting Vitalis Residentiële Woonvormen.
[3] Beleidsplan De Vitalis Zorg Groep 2003-2006.

beoordeeld. Het moge duidelijk zijn dat de gegevens die door Vitalis worden gebruikt ook persoonsgegevens bevatten, al waren het maar de naam en het adres van de afnemer.

Naast overeenkomsten met bewoners (de klanten van Vitalis) zijn er uiteraard de arbeidsovereenkomsten met de medewerkers. Ook bij de verwerking en nakoming van deze overeenkomst zullen, in de verschillende fasen voor, tijdens en na het sluiten van een arbeidscontract, persoonsgegevens worden verwerkt.

In de huidige maatschappij staat een dienstverlener als Vitalis niet alleen; financiers, overheid, relaties en leveranciers communiceren met de organisatie over een veelheid van zaken en vragen hierbij verantwoording voor geleverde diensten of producten. Ook in deze communicatie worden persoonsgegevens gebruikt, variërend van toetsingsgegevens voor vaststelling van de huursubsidie van een bewoner tot aan uitwisseling van medische gegevens met andere zorgsinstellingen en zelfs strafrechtelijke gegevens die noodzakelijk zijn bij dwangopnames.

Uit bovenstaande is duidelijk geworden dat De Vitalis Zorg Groep zowel voor haar klanten, haar medewerkers als ook voor andere betrokken partijen grote hoeveelheden persoonsgegevens vastlegt en verwerkt. Al deze verwerkingen zijn onderworpen aan de eisen die de WBP stelt. Welke verwerkingen op dit moment actueel zijn en of deze voldoen aan de eisen die door wettelijke regels worden gesteld, is onderwerp van dit onderzoek. De inventarisatie wordt behandeld in hoofdstuk 5, de toets op de eisen voor verwerking wordt uitgewerkt in hoofdstuk 6.

5 Inventarisatie bestaande gegevensverzamelingen

5.1 Inleiding

In dit hoofdstuk wordt beschreven welke informatieverwerkingen er binnen De Vitalis Zorg Groep worden gedaan. Het kader voor dit onderzoek is de WBP, de inventarisatie[4] richt zich daarom op die verwerkingen die voldoen aan de definities uit de WBP. Om te kunnen starten vanuit eenduidige definities zal de daadwerkelijke inventarisatie van verwerkingen voorafgegaan moeten worden door een korte beschrijving van de begrippen uit de WBP die de basis vormen voor de inventarisatie. De structuur die hiervoor zal worden gebruikt is die van de melding van verwerkingen aan het CBP. In dit hoofdstuk zullen, op basis van de onderwerpen die een melding moet bevatten, de relevante begrippen worden uitgewerkt en toegelicht.
Tijdens de daadwerkelijke uitvoering van het onderzoek zal met deze inventarisatie een dubbel doel gediend worden: enerzijds krijgt de organisatie het gewenste inzicht in de bestaande verwerkingen en anderzijds wordt hierdoor bereikt dat alle bestaande verwerkingen zijn aangemeld bij de functionaris gegevensbescherming waardoor mogelijk zondigen tegen de regels van de meldingsplicht is voorkomen.

5.2 De Wet Bescherming Persoonsgegevens als basis voor privacy

Het recht op bescherming van de persoonlijke levenssfeer, bescherming van de privacy, is vastgelegd in internationale verdragen, in Europese wetgeving, in de Nederlandse Grondwet en in de hierop gebaseerde wet- en regelgeving. Ook in het verdrag tot vaststelling van een Grondwet voor Europa[5] heeft de bescherming van privacy een eigen plaats gekregen in o.m. de artikelen II-67 (eerbiediging van het privé-leven en van het familie- en gezinsleven) en II-68 (bescherming van persoonsgegevens). Dit laatste artikel is gebaseerd op artikel 286 van het Verdrag tot oprichting van de Europese Gemeenschap en op Richtlijn 95/46/EG[6] van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, alsmede op artikel 8 van het EVRM en op het Verdrag van de Raad van Europa van 28 januari 1981 tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens[7]. Voorts wordt verwezen naar Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens[8]. Bovengenoemde richtlijn en verordening bevatten voorwaarden en beperkingen voor de uitoefening van het recht op bescherming van persoonsgegevens.

Startpunt voor dit onderzoek in deze inventarisaties van wet- en regelgeving is artikel 10 van de Grondwet waarin het recht op eerbiediging van de persoonlijke levenssfeer is vastgelegd. Dit recht kent in de zorg een drietal gedaanten: het recht op lichamelijke integriteit, het recht op bescherming van de ruimtelijke privacy en het recht op bescherming van informationele privacy wanneer verwerking van (medische) persoonsgegevens aan de orde is[9].
Omgang met (medische) persoonsgegevens wordt hoofdzakelijk gereguleerd door de WBP, waarbij de WBP de implementatie is van de eerder genoemde Europese richtlijn 95/46/EG en de opvolger van de Wet Persoonsregistraties (WPR). Tijdens de totstandkoming van de WBP zijn er discussies

[4] De stappen uit deze inventarisatie zijn gebaseerd op dezelfde stappen die werden aanbevolen bij de overgang van WPR naar WBP; zie voor deze stappenplannen o.a.: J. Holvast, Wet bescherming persoonsgegevens: overzicht en stappenplan, Privacy & Informatie, 1998, nr. 1 pag. 4 e.v, L.B. Sauerwein en J.J. Linneman, Handleiding voor verwerkers van persoonsgegevens, Den Haag, Ministerie van Justitie, 2001, pag. 7 e.v. en J. Nouwt, Invoering van de WBP in tien stappen, http://rechten.uvt.nl/sjaaknouwt/Zorgvisi.doc
[5] Verdrag tot vaststelling van een Grondwet voor Europa (met Protocollen, Bijlagen en Slotakte) Rome, 29 oktober 2004, Tractatenblad van het Koninkrijk der Nederlanden, Jaargang 2004, nr. 275.
[6] Richtlijn 95/46/EG van 23 november 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens, PbEG L281.
[7] http://www.grondweteuropa.nl/9326000/1/j9vvgjnazrhmix9/vgm7mnouggz9
[8] PbEG L8 van 12 januari 2001.
[9] J. Nouwt, Zorg voor privacy, informatietechnologie en informationele privacy in de gezondheidszorg, Den Haag, SDU, 1997, pag. 2.; H.J.J. Leenen, Handboek gezondheidsrecht deel 1: rechten van mensen in de gezondheidszorg, Houten, Bohn Stafleu van Loghum, 2000, pag. 248.

geweest over de noodzaak van specifieke privacywetgeving en of privacybescherming niet beter vanuit bestaande wetgeving zoals BW en Awb zou kunnen geschieden. Er is toch gekozen voor specifieke, bovensectorale wetgeving in de vorm van de WBP omdat, volgens de regering, privacywetgeving een nieuw rechtsgebied is dat het best tot zijn recht zal komen in een enkele wet[10].

Tussen de WPR en de WBP bestaat grote inhoudelijke continuïteit en weinig verschil in de verhouding van algemene tot bijzondere privacyregels, omdat beiden, evenals Richtlijn 95/46/EG, uitgaan van de grondbeginselen van het Verdrag van Straatsburg[11]. Tijdens de totstandkoming van de WBP is er zelfs door de regering gesteld dat de Richtlijn voortkomt uit de bundeling van nationale wetgeving waaronder de WPR, zodat het logisch is dat ook door deze constructie de WBP veel overeenkomsten heeft met de WPR.

De WBP geeft regels voor het verwerken van persoonsgegevens waarbij artikel 27 stelt dat een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens waaronder wordt verstaan elke handeling of samenstel van handelingen[12] met betrekking tot de verwerking van persoonsgegevens dient te worden gemeld bij het CBP[13] of de privacyfunctionaris. Deze melding moet worden gedaan voordat de verwerking begint, dus zelfs al voordat met het verzamelen van gegevens wordt begonnen. In principe behoeven alleen geautomatiseerde verwerkingen te worden gemeld. Gecombineerd met de uitgangspunten voor dit onderzoek impliceert dit dat handmatige verwerkingen, ook al zouden deze onder voorafgaand onderzoek zoals bedoeld in artikel 27 lid 2 WBP vallen, niet meegenomen worden in de inventarisatie en beoordeling. De melding van de verwerkingen zorgt voor openheid rond de verwerking van persoonsgegevens en stelt de betrokkenen in staat te controleren hoe hun gegevens worden verwerkt en om eventueel gebruik te maken van hun (wettelijke) rechten. Ook zorgt de meldingsplicht ervoor dat een effectief toezicht door het CBP mogelijk is. Overigens kan het CBP hierdoor in een rare dubbelrol terecht komen; enerzijds heeft het CBP een advies- en controlefunctie vooraf, anderzijds heeft het CBP de rol als wetshandhaver[14].

Zouden deze meldingscriteria onverkort worden gehanteerd, dan zou dit voor het College een forse administratieve belasting tot gevolg hebben. De wetgever achtte het daarom ook niet noodzakelijk om voor gegevensverwerkingen die algemeen bekend zijn en waarvan het onwaarschijnlijk is dat zij de persoonlijke levenssfeer van de betrokkene(n) schaden de meldingsplicht te handhaven[15]. In artikel 29, eerste lid, is daarom bepaald dat verwerkingen, waarvan het onwaarschijnlijk is dat deze inbreuk maken op de fundamentele rechten en vrijheden, zijn vrijgesteld van melding. Net zoals onder de “oude” WPR al het geval was, zijn een groot aantal verwerkingen van de meldingsplicht vrijgesteld. Deze vrijgestelde verwerkingen en de voorwaarden waaronder de vrijstelling van melding geldt, zijn opgenomen in het Vrijstellingsbesluit. Voldoet een verantwoordelijke niet aan de eisen uit het vrijstellingsbesluit of wil hij daarvan afwijken, dan zal de verwerking alsnog moeten worden aangemeld bij het CBP. De melding bij het CBP leidt echter niet automatisch tot een goedkeuring van de voorgenomen verwerking[16]. Bij handelen in strijd met hetgeen bij of krachtens de artikelen 27 of 28 is bepaald kan, volgens artikel 66, eerste lid, het CBP een bestuurlijke boete opleggen van € 4500,- per verwerking.

Het begrip “Vrijstellingsbesluit” wil in de taal van alledag nogal eens voor misverstanden zorgen omdat het begrip vrijstelling wordt geïnterpreteerd als vrijstelling van alle eisen van de WBP. De zorgvuldigheidseisen van de WBP blijven echter onverkort van toepassing op de verwerking van

[10] C. Cuijpers, Privacy of privaatrecht, een privaatrechtelijk alternatief voor de implementatie van de Europese privacyrichtlijn, Den Haag, SDU, 2004, pag. 13 e.v.
[11] Overgangsrecht WBP, Den Haag, CBP, 2001, pag. 1; http://www.cbpweb.nl/bis/content-1-14-12.html; J. Nouwt, WBP: veranderingen voor de zorgsector, in: Privacy en Informatie, 2000, nr. 3(2), pag. 65-70.
[12] Verwerkingshandelingen die in het maatschappelijk verkeer als eenheid worden gezien, behoeven niet als separate verwerkingen te worden aangemeld maar worden beschouwd als één verwerking. J. Nouwt, Invoering van de WBP in tien stappen, http://rechten.uvt.nl/sjaaknouwt/Zorgvisi.doc , pag. 3 en L.B. Sauerwein en J.J. Linneman, Handleiding voor verwerkers van persoonsgegevens, Den Haag, Ministerie van Justitie, 2001, pag. 31.
[13] Conform de bepalingen uit het Meldingsbesluit WBP (Besluit van 7 mei 2001, Stb. 244) en de Meldingsregeling WBP (Regeling van juli 2002, Stcrt. 137).
[14] In de literatuur wordt het verwijt aan het CBP gericht dat door deze vermenging van functies strijd ontstaat met het beginsel van functiescheiding waarbij (uiteraard) wordt verwezen naar het bekende Procola-arrest. Zie o.a. Kuitenbrouwer, Privacy, een historisch-vergelijkend overzicht in: J. Prins en J. Berkvens (red.), Privacyregulering in theorie en praktijk, Deventer, Kluwer, 2002, pag. 53-54.
[15] L.B. Sauerwein en J.J. Linneman, Handleiding voor verwerkers van persoonsgegevens, Den Haag, Ministerie van Justitie, 2001, pag. 32.
[16] D. Rijkers, Privacy, De Wet Bescherming Persoonsgegevens, Alphen aan den Rijn, Adformatie Groep, 2002, pag. 73.

gegevens, ook al is deze vrijgesteld van melding; vrijgestelde verwerkingen vallen dus gewoon onder de WBP[17].
Binnen de context van dit onderzoek is de verwachting dat de meeste van de actuele verwerkingen binnen Vitalis onder het Vrijstellingsbesluit vallen, maar het definitieve oordeel hierover zal pas geveld worden nadat de verwerkingen beschreven zijn, zowel de verwerkingen die reeds bestonden bij de inwerkingtreding van de WBP als de verwerkingen die daarna zijn gestart[18]. Binnen de uit te voeren inventarisatie zal dus vastgesteld moeten worden of en zo ja bij wie een verwerking is aangemeld en of dit conform de geldende voorwaarden is.

De melding van een verwerking, door of namens de verantwoordelijke, dient een aantal gegevens te bevatten op basis waarvan vastgesteld kan worden of de verwerking in aanmerking komt voor toepassing van het Vrijstellingsbesluit. Deze basisset van gegevens vormt binnen dit onderzoek de eerste stap in de inventarisatie van de verwerkingen bij De Vitalis Zorg Groep. Op elk van de gevraagde gegevens zal hieronder afzonderlijk dieper worden ingegaan, waarbij gebruik gemaakt wordt van de structuur zoals die door het CBP wordt aangeboden in het “Meldingsformulier verwerking persoonsgegevens”[19]. De gegevens die minimaal gemeld moeten worden zijn gegeven in artikel 25 WBP en luiden als volgt:

- naam / adres van de verantwoordelijke;
- doel of doeleinden van de gegevensverwerking;
- (categorieën van) betrokkenen;
- (categorieën van) gegevens van deze betrokkenen;
- (categorieën van) ontvangers;
- de voorgenomen doorgiften van persoonsgegevens aan landen buiten de Europese Unie; en
- een omschrijving van de door de verantwoordelijke te nemen of genomen beveiligingsmaatregelen.

Op de inhoudelijke consequenties van een eventuele vrijstelling van melding en de verdere eisen die de WBP aan verwerkingen stelt zal verderop in dit onderzoek (hoofdstuk 6) worden teruggekomen.

5.2.1 Wie is de verantwoordelijke?

Volgens artikel 1 sub d van de WBP is de verantwoordelijke degene, natuurlijke persoon of rechtspersoon, die het doel en de middelen van de verwerking vaststelt. Het gaat er bij dit begrip niet om wie de feitelijke beslissing tot verwerking neemt, maar wie de formeel bevoegde is om deze beslissingen te nemen[20]. Is bij het inventariseren niet helemaal duidelijk wie formeel-juridisch de bevoegdheid of de zeggenschap heeft, dan is er een tweede criterium om de verantwoordelijke vast te stellen: degene aan wie de verwerking, naar de maatstaven die in het maatschappelijke verkeer gelden, moet worden toegerekend[21]. Een aandachtspunt bij het vaststellen van de verantwoordelijke is nog de omstandigheid dat er meerdere belanghebbenden zijn bij een verwerking. In de toelichting bij de WBP zijn drie varianten van het begrip verwantwoordelijke beschreven[22]:

- Gezamenlijke verantwoordelijkheid; er is sprake van een aantal verantwoordelijken die in min of meer gelijke mate als verantwoordelijken voor het geheel van verwerkingen kunnen worden aangemerkt.
- Gedifferentieerde verantwoordelijkheid; er is sprake van meerdere verantwoordelijken waarbij elk een afgebakende, niet overlappende, verantwoordelijkheid voor een aantal bewerkingen heeft.

[17] WBP, Handleiding bij het invoeren van de wet bescherming persoonsgegevens, VOG, Utrecht, 2001, pag. 11.
[18] Als een verantwoordelijke van mening is dat een verwerking onder het Vrijstellingsbesluit valt, rust op hem de verplichting dit te onderbouwen. Een beschrijving van de verwerking in kwestie met de daarbij behorende argumenten die zouden moeten leiden tot vrijstelling van melding is dus noodzakelijk. Zie o.m. de overwegingen van de Rechtbank in Den Bosch, Sector bestuursrecht, AWB 04/1196 dd. 18 januari 2005. In dit geschil is de Gemeente Best beboet door het CBP voor het niet tijdig aanmelden van verwerkingen c.q. het niet voldoende onderbouwen van de aanspraak op vrijstelling van melding.
[19] www.cbpweb.nl
[20] J. Prins en J. Berkvens, De wet bescherming persoonsgegevens in: J. Prins en J. Berkvens (red.), Privacyregulering in theorie en praktijk, Kluwer, Deventer, 2002, pag. 85.
[21] L.B. Sauerwein en J.J. Linneman, Handleiding voor verwerkers van persoonsgegevens, Den Haag, Ministerie van Justitie, 2001, pag. 18.
[22] J. Prins en J. Berkvens, De wet bescherming persoonsgegevens in: J. Prins en J. Berkvens (red.), Privacyregulering in theorie en praktijk, Kluwer, Deventer, 2002, pag. 86.

- Gemeenschappelijke verantwoordelijkheid: hier is sprake van een aantal samenwerkende partijen die een derde belasten met het opzetten en onderhouden van gezamenlijke verwerkingen[23].

In concernverhoudingen waarbinnen verschillende rechtspersonen een rol spelen kan het moeilijk zijn een eindverantwoordelijke voor de verwerkingen te benoemen. In de aanloop naar de WBP is (naar analogie van het gebruik onder de WPR) de figuur van de concernverantwoordelijke ontstaan welke als verantwoordelijke voor alle verwerkingen in concernverband kan worden aangemerkt. Criterium voor het benoemen van de "holding" of andere overkoepelende rechtspersoon als concernverantwoordelijke is het feit of uit de statuten of onderlinge overeenkomsten kan worden afgeleid dat deze koepel of holding daadwerkelijk als verantwoordelijke binnen het concern mag worden aangemerkt[24]. Binnen de organisatie van de opdrachtgever is sprake van een drietal samenwerkende rechtspersonen die naar buiten treden als Stichting De Vitalis Zorg Groep. Binnen deze stichting zijn alle personeelsleden als ook alle bewoners administratief geplaatst, waardoor de facto alle verwerkingen binnen deze rechtspersoon plaatsvinden[25]. Deze stichting kan dus op basis van het begrip concernverantwoordelijke als verantwoordelijke voor alle verwerkingen van de dochters worden aangemerkt. Binnen het kader van dit onderzoek is de Raad van Bestuur van De Vitalis Zorg Groep de verantwoordelijke voor alle verwerkingen. Het apart inventariseren van de verantwoordelijke per verwerking is daarom niet noodzakelijk.

5.2.2 Is er een bewerker?

De mogelijkheid bestaat dat bepaalde verwerkingen van gegevens buiten de organisatie plaatsvinden, door derden in opdracht van de verantwoordelijke. Om te voorkomen dat door deze constructie bepaalde verantwoordelijkheden kunnen worden ontdoken introduceert de WBP in artikel 1 sub e het begrip "bewerker". Een bewerker verwerkt persoonsgegevens op last van de verantwoordelijke zonder aan diens rechtstreeks gezag te zijn onderworpen. Een voorbeeld van een bewerker is een bedrijf dat voor de instelling de salarisadministratie voert. De derde, de bewerker, heeft geen zeggenschap over de verwerking, maar handelt volgens de instructies en onder verantwoordelijkheid van de verantwoordelijke. Is er sprake van ondergeschiktheid of is er een andere vorm van hiërarchie met de verantwoordelijke, dan is er geen sprake meer van bewerker maar van (intern) beheerder[26].

5.2.3 Welke verwerking moet er gemeld worden?

Volgens de WBP valt elke handeling of elk samenhangend geheel van handelingen, van vastleggen tot en met vernietigen[27], met persoonsgegevens onder het begrip "verwerken", waarbij een aantal handelingen worden genoemd welke in ieder geval als verwerking(-shandeling) worden aangemerkt. Het begrip gegevensverwerking in de zin van de WBP omvat dus zowel het gehele proces dat een gegeven doormaakt vanaf het moment dat het wordt verkregen tot en met het moment dat het wordt vernietigd (verwerking in de zin van een samenhangend geheel van handelingen) alsook elke afzonderlijke technische of verwerkingshandeling in dit proces (verwerking in de enkelvoudige betekenis)[28]. De essentie is hier of de verwerker feitelijke macht of invloed kan uitoefenen op de verwerking; is dit niet het geval dan valt de verwerking niet onder de WBP[29]. Het is bij dit criterium overigens niet van belang of deze macht ook daadwerkelijk wordt uitgeoefend, als het maar mogelijk is[30].
De WBP is in ieder geval van toepassing op geautomatiseerde verwerking van gegevens[31]. Dit impliceert dat elk gebruik van een computer bij het verwerken van persoonsgegevens onder de WBP

[23] Het standaard voorbeeld dat bij deze vorm wordt gebruikt is dat van een ziekenhuis-informatiesysteem. Het ziekenhuis is verantwoordelijk voor het geheel en (externe) geneeskundigen die veranderingen aanbrengen in de informatie zijn verantwoordelijk voor deze mutaties.
[24] J. Prins en J. Berkvens, De wet bescherming persoonsgegevens in: J. Prins en J. Berkvens (red.), Privacyregulering in theorie en praktijk, Kluwer, Deventer, 2002, pag. 86.
[25] W. Slot d.d. 8 december 2004; De Vitalis Zorg Groep, Jaarverslag 2003, pagina 8, zie ook hoofdstuk 4.
[26] L.B. Sauerwein en J.J. Linneman, Handleiding voor verwerkers van persoonsgegevens, Den Haag, Ministerie van Justitie, 2001, pag. 19.
[27] S.M. Artz en L.E. van Laviere, De Wet bescherming persoonsgegevens, over de bescherming van uw persoonlijke gegevens, Den Haag, CBP, 2002, pag. 6.
[28] J. Prins en J. Berkvens, De wet bescherming persoonsgegevens in: J. Prins en J. Berkvens (red.), Privacyregulering in theorie en praktijk, Kluwer, Deventer, 2002, pag. 83.
[29] L.B. Sauerwein en J.J. Linneman, handleiding voor verwerkers van persoonsgegevens, Den Haag, Ministerie van Justitie, 2001, pag. 15.
[30] D. Rijkers, Privacy, De Wet Bescherming Persoonsgegevens, Alphen aan den Rijn, Adformatie Groep, 2002, pag. 19.
[31] J. Prins en J. Berkvens, De wet bescherming persoonsgegevens in: J. Prins en J. Berkvens (red.), Privacyregulering in theorie en praktijk, Kluwer, Deventer, 2002, pag. 84.

valt. Daarnaast vallen ook handmatig opgeslagen gegevens die met behulp van een computer gecatalogiseerd of toegankelijk gemaakt zijn onder verwerking. Ook handmatig opgeslagen gegevens die bestemd zijn om (te zijner tijd) opgenomen te worden in een geautomatiseerde verwerking vallen onder de werking van de WBP. De WBP is niet van toepassing op handmatig verwerkte persoonsgegevens die niet in een bestand zijn opgenomen en ook niet bestemd zijn om daarin te worden opgenomen. Onder bestand wordt verstaan een gestructureerd geheel van gegevens, ongeacht of dit geheel is gecentraliseerd of verspreid, dat volgens bepaalde criteria toegankelijk is en dat betrekking heeft op verschillende personen[32]. Hieruit kan afgeleid worden dat een bestand gegevens bevat die onderling moeten samenhangen en waarbij het (bestands-)systeem systematisch toegankelijk dient te zijn.

Voor de uit te voeren inventarisatie impliceert dit dat alle (computer)bestanden en programma's die binnen Vitalis in gebruik zijn onder het begrip verwerking vallen en dat deze, evenals alle lijsten c.q. overzichten die nog in de computer worden opgenomen, meegenomen moeten worden in de inventarisatie.

5.2.4 Wat is het doel van de verwerking?

Het uitgangspunt voor de Nederlandse privacywetgeving is artikel 6 WBP dat bepaalt dat verwerkingen van persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze dienen te worden verwerkt. De formulering "in overeenstemming met de wet" beperkt zich niet tot de WBP maar strekt zich ook uit tot eventuele andere wetgeving[33] (zoals hieronder verder uitgewerkt). Het begrip "zorgvuldig" kent zowel aansluiting met 6:162 BW voor wat betreft de civiele context als met het bestuursrechtelijke zorgvuldigheidsbeginsel voor wat betreft de publieke context.

De WBP geeft twee drempels die in chronologische volgorde genomen moeten worden alvorens met verwerking van persoonsgegevens kan worden begonnen: artikel 7 en artikel 8[34].
Artikel 7 schrijft voor dat verwerking slechts mag geschieden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen. Dit impliceert dat zonder duidelijke doelomschrijving vooraf geen persoonsgegevens mogen worden verwerkt maar tevens dat de vastgestelde doelen van de verwerking niet tijdens het proces mogen worden gewijzigd.
Artikel 8 is de uitwerking van de formulering "gerechtvaardigde doelen" uit artikel 7. Hierin zijn limitatief de gronden benoemd voor verwerking. Elke gegevensverwerking moet herleidbaar zijn tot een van de in dit artikel benoemde rechtvaardigingsgronden[35] en daarnaast uiteraard niet in strijd zijn met wet, openbare orde of goede zeden. Voor de zorgsector zal het verwerken van persoonsgegevens meestal gebaseerd worden op de onderdelen a (toestemming[36] van de patiënt of bewoner), b (overeenkomst tot geneeskundige behandeling, huur- of koopovereenkomst), c (wettelijke verplichting), d (vitaal belang van de betrokkene) of f (gerechtvaardigd belang van de verantwoordelijke)[37].

Nadat de bepalingen met betrekking tot doel en melding van de voorgenomen verwerking zijn doorlopen, gelden er nog aanvullende voorwaarden waaraan deze verwerking dient te voldoen. Artikel 9 stelt dat persoonsgegevens niet mogen worden verwerkt op een wijze die onverenigbaar is met het doel waarvoor zij zijn verkregen. In de praktijk betekent dit dat gegevens voor andere doelen mogen worden verwerkt, mits deze andere doelen voldoen aan de criteria uit het tweede lid: er moet een verwantschap zijn tussen het oorspronkelijke doel en het doel waarvoor de nieuwe verwerking geschiedt, er moet rekening gehouden worden met de aard en de wijze van verkrijgen van de gegevens en met de gevolgen van de voorgenomen verwerking voor betrokkene. Ook moeten er passende waarborgen jegens betrokkene worden getroffen. Deze formulering is tamelijk breed en zal

[32] R. van der Horst, De Wet bescherming persoonsgegevens, gevolgen voor de organisatie en de automatisering in: J. Prins en J. Berkvens (red.), Privacyregulering in theorie en praktijk, Kluwer, Deventer, 2002, pag. 105.
[33] L.B. Sauerwein en J.J. Linneman, Handleiding voor verwerkers van persoonsgegevens, Den Haag, Ministerie van Justitie, 2001, pag. 20-21.
[34] J. Nouwt, C. Louwerse, Algemene beginselen van gegevensverwerking, in: Handboek privacy in de zorg, Den Haag, Koninklijke Vermande, 2004, band 1, paragraaf 1.1.3.
[35] T.F.M. Hooghiemstra, Tekst en toelichting Wet bescherming persoonsgegevens, Koninklijke Vermande, 2003, pag. 63.
[36] Toestemming moet aan een aantal criteria voldoen: betrokkene moet zijn wil in vrijheid hebben geuit, de toestemming van betrokkene moet gericht zijn op bepaalde gegevensverwerkingen en de toestemming moet ondubbelzinnig zijn. Zie L.B. Sauerwein en J.J. Linneman, Handleiding voor verwerkers van persoonsgegevens, Den Haag, Ministerie van Justitie, 2001, pag. 22.
[37] J. Nouwt, WBP: veranderingen voor de zorgsector, in: Privacy en Informatie, 2000, nr. 3(2), pag. 65.

sterk feitelijk moeten worden ingevuld. Ook andere factoren dan hier genoemd kunnen een rol spelen bij het bepalen van de verenigbaarheid van de doelen en het is niet zo dat één factor per definitie zwaarder weegt dan een andere[38].

Lid 3 van artikel 9 is concreter: verwerking voor wetenschappelijke doeleinden, voor zover niet het oorspronkelijke doel, is toegestaan onder bepaalde voorwaarden. Lid 4 is het meest duidelijk: indien een geheimhoudingsplicht het belet, is verwerking niet toegestaan. In de context van dit onderzoek betekent dit dat geen persoonsgegevens mogen worden verwerkt indien dit strijdig zou zijn met het medisch beroepsgeheim.

Naast het vaststellen van de (sub)doelen van de verwerking is het van belang hieronder ook een toets uit te voeren op de herkomst van de verwerkte gegevens. Het inventariseren van de herkomst van de gegevens is belangrijk omdat de herkomst van de gegevens in overeenstemming moet zijn met het doel van de verwerking. Gegevens die voor een ander doel verkregen zijn, mogen niet zondermeer worden verwerkt[39]. Binnen de inventarisatie zal dus duidelijkheid moeten ontstaan over de herkomst van de gegevens zodat in een later stadium de vergelijking met het opgegeven doel van de verwerking kan worden gemaakt. Ook zal de organisatie zich bewust moeten zijn van de verplichting om vooraf de doelen van de verwerking te formuleren en vast te leggen.

5.2.5 Van welke betrokkenen worden gegevens verwerkt?

Een logische stap is een verdeling in de gevonden verwerkingen naar betrokkenen, degenen van wie persoonsgegevens worden verwerkt. Het initiële onderscheid kan hier gemaakt worden op basis van de primaire groepen betrokkenen waarmee een zorginstelling als Vitalis te maken heeft. Een praktisch onderscheid is uiteraard de verdeling naar patiënt/cliënt gerelateerde verwerkingen tegenover personeelsgerichte verwerkingen. Deze twee hoofdgroepen kunnen verder worden verdeeld in patiënten/cliënten, personen uit de omgeving van de patiënt/cliënt zoals vertegenwoordigers, eigen personeel en hulpverleners buiten de organisatie[40]. Een nauwkeurige verdeling en beschrijving van de betrokkenen is van belang omdat hier andere wettelijke eisen zoals de informatieplichten en het recht op verzet, inzage en correctie aan zijn gerelateerd.

5.2.6 Welke persoonsgegevens worden verwerkt?

Kernbegrip uit de WBP en dus ook voor de inventarisatie is het begrip “persoonsgegeven”; de bepalingen uit de WBP zijn slechts van toepassing als het gaat om (het verwerken van) persoonsgegevens. Gegevens zijn persoonsgegevens als de gegevens informatie bevatten over een natuurlijke persoon en die persoon identificeerbaar is (art 1 WBP); de WBP noemt de persoon van wie persoonsgegevens verwerkt worden de betrokkene.

Of de gegevens informatie geven over een natuurlijke persoon hangt sterk af van de aard van de gegevens. Gegevens die feitelijke informatie over een persoon geven vallen wel onder de WBP. Gegevens over organisaties of ondernemingen welke geen betrekking hebben op natuurlijke personen vallen in principe niet onder de WBP tenzij er gegevens over contactpersonen in worden opgenomen of de gegevens medebepalend zijn voor de manier waarop een individu wordt beoordeeld of behandeld in het maatschappelijk verkeer. Een zelfde redenering gaat op voor gegevens over voorwerpen; staan deze op zichzelf (de prijs van een auto in een catalogus) dan zijn het geen persoonsgegevens. Is dit zelfde gegeven herleidbaar tot een natuurlijk persoon (de prijs van de auto als basis voor mijn verzekeringspolis) dan is het weer wel een persoonsgegeven en valt het onder de WBP[41].

[38] L.B. Sauerwein en J.J. Linneman, Handleiding voor verwerkers van persoonsgegevens, Den Haag, Ministerie van Justitie, 2001, pag. 26.
[39] WBP, Handleiding bij het invoeren van de wet bescherming persoonsgegevens, VOG, Utrecht, 2001, pag. 22.
[40] Zie voor deze basisverdeling de suggesties uit: WBP, handleiding bij het invoeren van de Wet bescherming persoonsgegevens, VOG, Utrecht, 2001, pag. 19.
[41] Voorbeelden ontleend aan: J. Prins en J. Berkvens, De wet bescherming persoonsgegevens in: J. Prins en J. Berkvens (red.), Privacyregulering in theorie en praktijk, Kluwer, Deventer, 2002, pag. 81.

De volgende eis die art 1 van de WBP aanlegt is die van identificeerbaarheid[42] van de persoon: een persoon is identificeerbaar als de identiteit van de persoon redelijkerwijs en zonder onevenredige inspanning kan worden vastgesteld. Een naam hoeft dus niet eens deel uit te maken van de beschikbare gegevens zo lang de persoon maar identificeerbaar is. Van herleidbaarheid (en dus van een persoonsgegeven) is geen sprake indien een onevenredige hoeveelheid tijd, geld en mankracht nodig zou zijn om een herleiding van het gegeven naar een bepaalde persoon te bewerkstelligen[43].

Samenvattend kan gesteld worden dat persoonsgegevens dus alle gegevens zijn die iets over een persoon zeggen en die van invloed kunnen zijn op de manier waarop een persoon wordt beoordeeld en behandeld[44]. Een persoonsgegeven verschaft direct of indirect informatie over een persoon en deze persoon moet redelijkerwijs direct of indirect identificeerbaar zijn. Dit vormt het eerste uitgangspunt voor de inventarisatie, maar is nog te abstract om te gebruiken in de inventarisatie; de verschillende categorieën persoonsgegevens dienen concreter benoemd te worden.

Binnen de structuur van de uit te voeren inventarisatie is de volgende verfijning, naast een primaire verdeling in betrokkenen zoals beschreven in paragraaf 5.2.5, het verdelen van de persoonsgegevens in algemene persoonsgegevens en bijzondere gegevens, een onderscheid dat ook door de WBP al gemaakt wordt[45]. Binnen de algemene persoonsgegevens kan een verdere verdeling worden gemaakt in personalia of identificerende gegevens en financieel-administratieve gegevens[46]. Onder bijzondere persoonsgegevens vallen de medische en sociaal-psychologische gegevens, gegevens betreffende godsdienst of levensovertuiging, gegevens met betrekking tot ras en etniciteit, gegevens die betrekking hebben op het seksuele leven alsmede strafrechtelijke gegevens of persoonsgegevens die betrekking hebben onrechtmatig of hinderlijk gedrag naar aanleiding waarvan een verbod is opgelegd[47].

Binnen dit onderzoek zullen binnen de verwerkingen dan ook de volgende gegevens worden geïnventariseerd:

- Persoonlijke- of identificerende gegevens (PI);
- Financieel-administratieve gegevens (FA);
- Medische- en sociaal-psychologische gegevens (MSP);
- Gegevens met betrekking tot ras en etniciteit (RE);
- Gegevens met betrekking tot godsdienst en/of levensovertuiging (GLO);
- Strafrechtelijke gegevens of gegevens die betrekking hebben op onrechtmatig of hinderlijk gedrag (SOH).

5.2.7 Ontvanger?

De WBP verstaat hieronder degene aan wie persoonsgegevens worden verstrekt, binnen of buiten de eigen organisatie. Dit begrip is erg ruim; er vallen niet alleen personen, afdelingen of instanties onder die van anderen persoonsgegevens krijgen aangeleverd maar ook personen die op basis van hun functie een of andere vorm van toegang hebben tot de gegevensverwerkingen. Om dit begrip bruikbaar te maken voor de geplande inventarisatie van bestaande verwerkingen, dient dit verder geconcretiseerd te worden. Onderstaande rollen[48] geven een bruikbare onderverdeling van het begrip ontvanger.

Gebruiker
Uiteraard worden persoonsgegevens vastgelegd met het doel ze te gebruiken. Ook de gebruiker is dus een relevante actor die beschreven moet worden tijdens de inventarisatie. Een gebruiker hoeft niet noodzakelijkerwijs een individu te zijn, maar kan ook een groep of een afdeling zijn. In

[42] Richtlijn EU 95/46/EG geeft in art 2 sub 2 als voorbeeld de volgende mogelijkheden: identificatie aan de hand van een identificatienummer of een of meer specifieke elementen die kenmerkend zijn voor zijn of haar fysieke, fysiologische, psychische, economische, culturele of sociale identiteit.
[43] J. Nouwt, Zorg voor privacy, informatietechnologie en informationele privacy in de gezondheidszorg, Den Haag, SDU, 1997, pag. 2.126.
[44] S.M. Artz en L.E. van Laviere, De Wet bescherming persoonsgegevens, over de bescherming van uw persoonlijke gegevens, Den Haag, CBP, 2002, pag. 2.
[45] Zie paragraaf 2 WBP.
[46] J. Nouwt, WBP: veranderingen voor de zorgsector, in: Privacy en Informatie, 2000, nr. 3(2), pag. 65.
[47] De opsomming uit artikel 16 WBP
[48] Deze rollen zijn afgeleid uit de voorbeelden die gebruikt worden in de Toelichting bij het Meldingsformulier verwerking persoonsgegevens; CBP, Den Haag,

tegenstelling tot de bewerker staat de gebruiker wel onder gezag van de verantwoordelijke. Niet alleen wie de gebruiker is, is relevant, maar ook wat de gebruiker met de persoonsgegevens kan doen: invoeren, inzien, muteren, verwijderen[49] etc. Een nauwkeurige omschrijving van de bevoegdheden van de gebruikers is van belang om later de organisatorische maatregelen die genomen zijn of moeten worden om onbevoegde verwerking tegen te gaan uit te werken.

Beheerder
Naast de verantwoordelijke is het van belang te weten wie er de dagelijkse zorg voor de verwerkingen heeft, niet alleen voor de geautomatiseerde, maar ook voor de papieren dossiers. Meestal zal dit een afdelingshoofd of een groepsleider zijn. Per verwerking is er meestal maar één beheerder, maar een organisatie kan dus meerdere beheerders voor verschillende verwerkingen hebben[50]. Dit kenmerk van een verwerking is van belang omdat in de praktijk de beheerder het eerste aanspreekpunt van de betrokkene zal zijn, de contactpersoon voor deze verwerking. Vanuit deze rol speelt de beheerder, zeker als het een leidinggevende is, vaak een rol bij het regelen van de toegang tot de verwerking door andere gebruikers.

Derde(n)
Deze restcategorie omvat allen die, niet zijnde betrokkenen, verantwoordelijken, bewerkers of enig ander persoon onder rechtstreeks gezag van de verantwoordelijke of de bewerker, gemachtigd zijn persoonsgegevens te verwerken.

5.2.8 Voorgenomen buitenlandse verstrekkingen?

Het is toegestaan om medische hulp in het buitenland te zoeken voor bijvoorbeeld een bril, tandheelkundige hulp of zelfs (hart)transplantaties, dus ook voor bewoners van Vitalis. Uiteraard zal zich in deze gevallen de noodzaak voordoen van uitwisseling van (medische) persoonsgegevens met het buitenland. Binnen de EU is dit geen probleem, maar persoonsgegevens mogen in principe slechts doorgegeven worden naar landen buiten de EU indien deze een voldoende niveau van bescherming garanderen[51]. Op grond van artikel 77 van de WBP kunnen ook persoonsgegevens doorgegeven worden naar landen buiten de EU die niet over een passend beschermingsniveau beschikken indien voldaan is aan een aantal voorwaarden.
Voor de enquête zal dus moeten worden geïnventariseerd of binnen de opgegeven verwerking gegevens worden doorgegeven naar het buitenland en zo ja, aan welk land.

5.2.9 Beveiliging?

Beveiligingsmaatregelen kunnen in drie soorten worden onderscheiden. Ten eerste vallen daar de geheimhoudingsplichten op grond van beroep, ambt, wettelijk voorschrift of contract onder. Een tweede beveiligingsmaatregel betreft het nemen van passende technische en organisatorische maatregelen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Ten derde is de verantwoordelijke ook verantwoordelijk voor de deugdelijkheid van de beveiligingsmaatregelen die de bewerker neemt. De verantwoordelijke heeft de zorgplicht om de bewerker voldoende duidelijk te maken hoe met de persoonsgegevens moet worden omgegaan en dient toe te zien op de feitelijke naleving van deze verplichtingen[52].
Naast aandacht voor beveiliging in de meldingsprocedure is afdoende beveiliging ook een eis die voortdurend aan bestaande verwerkingen moet worden gesteld. In deze paragraaf zal dan ook worden volstaan met de vaststelling dat een omschrijving van de genomen maatregelen deel uitmaakt van de melding en de inhoudelijke uitwerking van de diverse aspecten van beveiliging van persoonsgegevens vindt plaats in paragraaf 6.6. Hier zal blijken dat de open norm uit artikel 13 WBP de organisatie constant met grote onzekerheid omtrent de naleving van de wet zal confronteren.

5.2.10 Artikel 2 lid 2 WBP: uitzonderingen

De bovenstaande kernbegrippen persoonsgegevens, verwerken en bestand vormen de basis voor de inventarisatie binnen Vitalis. Alle verwerkingen die aan deze criteria voldoen dienen in principe te

[49] WBP, Handleiding bij het invoeren van de wet bescherming persoonsgegevens, VOG, Utrecht, 2001, pag. 21.
[50] J. Nouwt, Invoering van de WBP in tien stappen, http://rechten.uvt.nl/sjaaknouwt/Zorgvisi.doc , pag. 2 en WBP, Handleiding bij het invoeren van de wet bescherming persoonsgegevens, VOG, Utrecht, 2001, pag. 21.
[51] J. Nouwt, Invoering van de WBP in tien stappen, http://rechten.uvt.nl/sjaaknouwt/Zorgvisi.doc , pag. 4.
[52] J. Nouwt, Invoering van de WBP in tien stappen, http://rechten.uvt.nl/sjaaknouwt/Zorgvisi.doc , pag. 3 en WBP, Handleiding bij het invoeren van de wet bescherming persoonsgegevens, VOG, Utrecht, 2001, pag. 14-15.

worden geïnventariseerd om te voldoen aan de onderzoeksdoelstelling. Alvorens daadwerkelijk te starten is het noodzakelijk aandacht te besteden aan artikel 2 van de WBP dat een aantal verwerkingen van de werkingssfeer van de WBP uitzondert: deze wet is niet van toepassing op verwerkingen ten behoeve van persoonlijk of huishoudelijk gebruik en niet van toepassing indien de verwerking valt onder een van de aangewezen, benoemde uitzonderingen.
Onder de eerste uitzondering vallen o.a. persoonlijke aantekeningen of adresbestanden die slechts door één persoon en voor zichzelf worden gebruikt. Deze hebben het karakter van persoonlijke aantekeningen, dienend als geheugensteun en zijn dus uitgezonderd van de werking van de WBP[53].

De gevolgen voor de uit te voeren inventarisatie van verwerkingen is dat persoonlijke documenten, lijstjes en overzichten van individuele netwerkgebruikers, ook al zijn het bestanden en bevatten ze persoonsgegevens, niet meegenomen hoeven te worden.

5.3 Praktische structuur voor het inventariseren van de verwerkingen.

Om met de geïnventariseerde verwerkingen verder te kunnen werken is het noodzakelijk dat het verzamelen gestructureerd kan gebeuren. Het opzetten[54] van een logische structuur die gebruikt wordt om de interviews voor de inventarisatie af te nemen is daarom relevant. De basisstructuur van de inventarisatie is gebaseerd op de begrippen uit de WBP zoals deze in artikel 1 zijn gedefinieerd. Deze begrippen zullen worden gebruikt om per rol van Vitalis een invulling te geven. De twee hoofdrollen die door Vitalis worden vervuld zijn die van zorgverlener en die van werkgever. Alvorens dus gestart kan worden, is het noodzakelijk een verdeling te maken in de (zorg)producten die door de organisatie geleverd worden en daarnaast een verdeling in de producten die Vitalis als werkgever aan haar personeel levert.

Gezien de achtergrond van de organisatie is een verdeling naar “zorgproducten” uit de AWBZ[55] een voor de hand liggende keuze, niet alleen voor het deel van de organisatie dat vanuit de AWBZ wordt gefinancierd, maar ook voor andere onderdelen; het geleverde productenpakket is immers in principe hetzelfde. Toepassen van dit criterium resulteert in de volgende verdeling:

- persoonlijke verzorging
- huishoudelijke verzorging
- verpleging
- ondersteunende begeleiding
- activerende begeleiding
- behandeling
- verblijf

Binnen deze basisverdeling is het goed om een verdere verdeling te ontwerpen, enerzijds wordt hiermee bereikt dat tijdens het inventariseren geen aandachtsgebieden worden overgeslagen, anderzijds kan hiermee later in het onderzoek makkelijker tussen de verschillende locaties van Vitalis worden vergeleken.

Voor het beschrijven van verwerkingen met betrekking tot personeel wordt aansluiting gezocht bij de “fasen van de loopbaan”: sollicitant, uitzendkracht c.q. gedetacheerde, vrijwilliger, vast personeel waarbij zieke en arbeidsongeschikte werknemers een aparte categorie vormen, ex-werknemers, gepensioneerden / OBU[56].

[53] Zie o.a. E.M. Crebas et al (red.), Handboek Privacy in de gezondheidszorg, Band 2, Paragraaf B.1, Reikwijdte WBP, Den Haag, Koninklijke Vermande, 2002, en L.B. Sauerwein en J.J. Linneman, handleiding voor verwerkers van persoonsgegevens, Den Haag, Ministerie van Justitie, 2001, pag. 17.
[54] De gebruikte structuur voor het opzetten van interviews is afkomstig uit: B. Emans, Interviewen, theorie, techniek en training, Groningen, Wolters-Noordhoff, 1990, pag. 110 e.v.
[55] De AWBZ is een verplichte verzekering voor de gehele bevolking tegen ziektekosten die niet via het ziekenfonds of de particuliere verzekering worden gedekt. Wanneer men voldoet aan een aantal wettelijke criteria is men van rechtswege verzekerd. Men is dan tevens verplicht om de wettelijke premie te betalen. Zie o.a. P. Wieringa en M. van den Toorn (red.), Jaaroverzicht Zorg, pag. 38-39, in: Handboek Privacy in de gezondheidszorg, Den Haag, Koninklijke Vermande, 2004.
[56] Deze verdeling is afgeleid van paragraaf 2 van het Besluit van 7 mei 2001, houdende aanwijzing van verwerking van persoonsgegevens die zijn vrijgesteld van melding bedoeld in artikel 27 van de Wet bescherming persoonsgegevens (Vrijstellingsbesluit WBP).

5.4 Samenvatting: overzicht te inventariseren gegevens

Als alle onderdelen uit voorgaande paragrafen worden samengebracht, resulteert dit in onderstaand overzicht:

1. Beheerder; wie heeft de dagelijkse zorg voor de verwerking, wie is het eerste aanspreekpunt?
2. Hoe is de naam of omschrijving van de verwerking en voor welke dienst / product worden deze gegevens verwerkt?
    a. AWBZ-produkten + omschrijving of productnaam,
    b. Personeel,
3. Met welk doel en op welke grondslag worden de gegevens verzameld?
4. Wie is de betrokkene, van/over wie worden gegevens verwerkt?
    a. Patiënt / bewoner,
    b. Relatie van patiënt of bewoner,
    c. Externe hulpverlener
    d. Sollicitant,
    e. Personeelslid,
    f. Ziek of arbeidsongeschikt personeelslid,
    g. Uitzendkracht c.q. gedetacheerde,
    h. Vrijwilliger,
    i. Ex-personeelslid,
    j. Gepensioneerde / OBU.
5. Welke categorieën van gegevens worden verwerkt?
    a. Persoonsgegevens:
        i. Persoonlijke- of identificerende gegevens (PI);
        ii. Financieel-administratieve gegevens (FA);
    b. Gevoelige gegevens:
        i. Medische- en sociaal-psychologische gegevens (MSP);
        ii. Gegevens met betrekking tot ras en etniciteit (RE);
        iii. Gegevens met betrekking tot godsdienst en/of levensovertuiging (GLO);
        iv. Strafrechtelijke gegevens of gegevens die betrekking hebben op onrechtmatig of hinderlijk gedrag (SOH).
6. Bewerker; indien gegevens buiten de organisatie verwerkt worden, door wie?
7. Aan wie worden de gegevens verstrekt?
    a. Gebruikers; wie gebruikt de gegevens en op welke manier?
    b. Beheerders,
    c. Derden; worden gegevens gebruikt of verwerkt door anderen dan de hierboven genoemde actoren en zo ja, door wie
8. Herkomst gegevens; hoe zijn de gegevens verkregen en past de herkomst van de gegevens bij het opgegeven doel van de verwerking?
9. Toelichting m.b.t. de genomen beveiligingsmaatregelen van de verwerking.
10. Voorgenomen buitenlandse doorgiften.
11. Melding; is deze verzameling al eerder aangemeld bij het CBP of de FG?
12. Aanvullende omschrijving over de werking van de beschreven verwerking of verwerkingshandelingen.

Mat behulp van deze lijst, die de helft vormt van de uiteindelijke enquête zullen de bestaande verwerkingen in kaart worden gebracht. Naast deze inhoudelijke kenmerken van verwerkingen, stelt de WBP ook eisen en voorwaarden waaronder verwerkt mag worden. Nu de verschillende kenmerken van verwerkingen beschreven zijn, wordt in het volgende hoofdstuk ingegaan op de eisen die hieraan gesteld worden. De combinatie hiervan zal leiden tot een enquêtevorm waarin de organisatie per verwerking de kenmerken en de voorwaarden die gelden voor verwerking kan aangeven

6 Vaststellen eisen aan gevonden verwerkingen

6.1 Inleiding

Nu het fundament voor het inventariseren van verwerkingen is gelegd, kan per verwerking worden vastgesteld wat de eisen zijn waaraan deze verwerking moet voldoen. De basis waarop deze beoordeling zal plaatsvinden, wordt gevormd door de algemene beginselen van privacy zoals deze ten grondslag liggen aan de huidige wettelijke bescherming van privacy. Deze beginselen vormen zowel de basis voor de Europese Richtlijn 95/46 als ook voor de nationale wetgeving. Deze beginselen, voor het eerst geformuleerd door de OESO in de *Guidelines for protection of privacy and transborder flows of personal data*, zijn specifiek van toepassing op de bescherming van persoonsgegevens (informationele privacy) en niet op andere vormen van privacybescherming[57] (lichamelijke, ruimtelijke en relationele privacy). Deze beginselen zijn in twee groepen te verdelen: de eerste groep heeft betrekking op de verwerkte gegevens als zodanig en de voorwaarden waaronder ze verwerkt mogen worden en de tweede groep heeft betrekking op de verplichtingen van de verwerker en de rechten van de betrokkenen[58].
Specifiek voor toetsing van privacybescherming bij gebruik van ICT in de zorg zijn deze algemene beginselen, via de beginselen uit de WBP, vertaald in zes algemene beginselen: transparantie, doelbinding, rechtmatige grondslag voor verwerking, kwaliteit van de gegevens, beveiliging en bewaartermijnen[59]. Vanuit deze zes beginselen worden de geïnventariseerde verwerkingen beoordeeld, maar om deze eisen te concretiseren en verderop in dit onderzoek ook meetbaar te maken, is de WBP niet meer dan een kader van waaruit de specifiek technische en organisatorische normen moeten worden afgeleid[60]. De concrete voorwaarden waaraan verwerkingen moeten voldoen worden vaak gegeven door een veelheid, van de WBP afgeleide of hieraan gerelateerde, wetten en besluiten.

Deze relevante wet- en regelgeving zal, per beginsel, worden verdeeld in een aantal hoofdcategorieën. Allereerst zal worden gekeken of een verwerking is vrijgesteld van melding zodat de extra bepalingen uit het Vrijstellingsbesluit van toepassing zijn. A contrario redenerend kan een niet gemelde verwerking ook getoetst worden aan dit besluit; de verwerking is immers niet gemeld en moet dus voldoen aan de bepalingen uit het Vrijstellingsbesluit. Zoals reeds eerder opgemerkt zou afzonderlijke aanmelding van alle mogelijke gegevensverwerkingen leiden tot een overbelasting van het College, reden waarom onder de WBP, via het bepaalde in artikel 27, vele vrijstellingen van deze meldingsplicht zijn gegeven. Het gaat bij deze, van melding vrijgestelde, verwerkingen om allerlei standaardregistraties die worden omschreven in het Vrijstellingsbesluit. Voor de zorgsector zijn verschillende vrijstellingen relevant. Voor de verwerking van bewoners- c.q. cliëntgegevens zijn de belangrijkste[61] de verwerking van gegevens van bewoners van verzorgings- en verpleeghuizen (art 17 Vrijstellingsbesluit), verwerking door beroepsbeoefenaren in de individuele gezondheidszorg (artikel 16 Vrijstellingsbesluit), verwerkingen die uitsluitend een archiefbestemming hebben (artikel 29 Vrijstellingsbesluit) en verwerkingen in verband met de behandeling van bezwaarschriften en klachten (artikel 39 Vrijstellingsbesluit).

[57] J. Nouwt, C.P. Louwerse, Algemene beginselen van gegevensverwerking in: Handboek Privacy in de gezondheidszorg, Den Haag, Koninklijke Vermande, 2004, Band 1, hoofdstuk 1.1, pag. 7 e.v.
[58] Eerste groep: Collection Limitation Principle, Data Quality Principle, Purpose Specification Principle en Use Limitation Principle. Tweede groep: Security Safeguard Principle, Openness Principle, Individual Participation Principle, Accountability Principle. Zie J. Nouwt, C.P. Louwerse, Algemene beginselen van gegevensverwerking in: Handboek Privacy in de gezondheidszorg, Den Haag, Koninklijke Vermande, 2004, Band 1, hoofdstuk 1.1, pag. 8 e.v.; J. Nouwt, Zorg voor privacy, informatietechnologie en informationele privacy in de gezondheidszorg, Den Haag, SDU, 1997, pag. 31 en 320 e.v.; F. Kuitenbrouwer, Privacy: een historisch-vergelijkend overzicht in: J. Prins en J. Berkvens (red.), Privacyregulering in theorie en praktijk, Deventer, Kluwer, 2002, pag. 43.
[59] T.F.M. Hooghiemstra, Privacy bij ICT in de Zorg. Bescherming van persoonsgegevens in de informatiestructuur van de gezondheidszorg, Den Haag, CBP, 2002, pag. 35.
[60] Vanuit deze benadering lijkt het alsof bescherming van de privacy afhankelijk is van de administratieve voorschriften die omgang met persoonsgegevens reguleren. Omgang met persoonsgegevens is slechts een onderdeel van privacybescherming maar door de nadruk van de WBP op administratieve bescherming ontstaat het risico dat inhoudelijke bescherming van het individu tegen de gevolgen van ongeautoriseerde verwerking onvoldoende aandacht krijgt. Zie voor vergelijkbare kritiek Kuitenbrouwer, Privacy, een historisch-rechtsvergelijkend overzicht in: J. Prins en J. Berkvens (red.), Privacyregulering in theorie en praktijk, Deventer, Kluwer, 2002, pag. 54 en C. Cuijpers, Privacy of privaatrecht, SDU, 2004, pag. 12-15. Ook het Rathenau Instituut heeft vergelijkbare kritiek geuit in het Bericht aan het Parlement van augustus 1998.
[61] J. Nouwt, WBP: veranderingen voor de zorgsector, in: Privacy en Informatie, 2000, nr. 3(2), pag. 66.

Ook voor verwerking van gegevens van personeel werkzaam in de zorgsector bestaan vrijstellingen in de aanmeldingsplicht. Het gaat hierbij o.a. om[62] verwerking van gegevens over sollicitanten (artikel 5), verwerkingen van gegevens over personeelsleden en uitzendkrachten (artikel 6, 7, 8 en 9), oud-personeelsleden (artikel 10). Naast deze verwerkingen is er nog een aantal vrijgesteld van melding die te vatten zijn onder het begrip “gegevens voor het interne beheer van de organisatie” (artikel 36). Voor de organisatie kunnen hier nog aan toegevoegd worden de verwerkingen van gegevens betreffende leveranciers en afnemers c.q. debiteuren en crediteuren (artikel 12 en 13), huur en verhuur van onroerende zaken voor zover niet vallende onder de woonzorg-bepalingen uit artikel 17 (artikel 14), toegang en beheer van computer-, netwerk- en telecommunicatiesystemen en gebouwen (artikel 33, 32, 34 en 35).
Binnen al deze bepalingen worden concrete voorwaarden gegeven met betrekking tot het toegestane doel van de verwerking, welke gegevens mogen worden verwerkt, aan wie deze gegevens mogen worden verstrekt en hoe lang de gegevens mogen worden bewaard[63].

Indien het Vrijstellingsbesluit onvoldoende houvast geeft of de verwerking is niet vrijgesteld van melding, zal de verwerking worden getoetst aan geldende sectorale wetgeving, wetgeving die speciaal voor de zorgsector is ontwikkeld en waarbij privacybepalingen onderdeel zijn van de regelgeving. Een van de belangrijkste wetten die hierbij van toepassing zijn is de WGBO. De verhouding tussen WBP en WGBO is er een van wederzijdse aanvulling, waarbij de specifieke bepalingen uit het BW als lex specialis voorgaan op het gestelde in de WBP[64]. Op grond van artikel 9 lid 4 gaan bijvoorbeeld de wettelijke bepalingen omtrent het (medisch) beroepsgeheim uit de WGBO (7:457 en 7:458 BW) voor[65] op de bepalingen van de WBP[66]. Deze sectorale wetgeving wordt, indien nodig, uitgebreid met controle op privacybepalingen in andere (horizontale) wetgeving[67].

Zoals reeds in het begin aangegeven, zal ook moeten worden gekeken naar mogelijk geldende gedragscodes voor de zorgsector die op grond van artikel 25 WBP zijn opgesteld en goedgekeurd. Ten slotte kunnen ook op grond van artikel 26 WBP bij Algemene maatregelen van bestuur nadere regels worden gesteld voor invulling van de artikelen 6 tot en met 11 en 13.

6.2 Transparantie

Het gaat bij het transparantiebeginsel om het uitgangspunt dat de betrokkene i.c. de patiënt/cliënt en/of de hulpverlener op de hoogte is van het feit dat er persoonsgegevens over hem worden verwerkt en met welk doel *(openness principle)* en dat betrokkenen hierover wordt geïnformeerd. Om dit te kunnen vaststellen is het van belang te weten waar, wanneer en door wie persoonsgegevens worden verwerkt. Dit uitgangspunt is vastgelegd in zowel het Verdrag van Straatsburg (art 8[68]), de OESO[69]-privacyrichtlijn[70] (art 12), de EU-privacyrichtlijn (artikelen 10, 11 en 12) en ook in het verdrag tot vaststelling van een Europese Grondwet (artikel II-68, zie ook paragraaf 5.2). Het betreft hier het recht

[62] J. Nouwt, WBP: veranderingen voor de zorgsector, in: Privacy en Informatie, 2000, nr. 3(2), pag. 66.
[63] Binnen de systematiek van de artikelen uit het Vrijstellingsbesluit meestal in respectievelijk sub 2, sub 3, sub 4 en sub 5.
[64] Het adagium: lex specialis derogat legi generalis. H.J.J. Leenen, Handboek gezondheidsrecht deel 1: rechten van mensen in de gezondheidszorg, Houten, Bohn Stafleu van Loghum, 2000, pag. 254.
[65] Zie NJ2001/600: geheimhoudingsplicht is sterker dan informatieplicht aan erfgenamen.
[66] T.F.M. Hooghiemstra, Tekst en toelichting Wet bescherming persoonsgegevens, Koninklijke Vermande, 2003, pag. 31.
[67] Zoals de wet BOPZ, de wet afbreking zwangerschap, wet tarieven gezondheidszorg, de wet medisch wetenschappelijk onderzoek etc. Als deze regels geven, ter bescherming van de privacy, aan dat de te verstrekken of te verwerken gegevens niet tot individuele patiënten of cliënten herleidbaar mogen zijn. Zie H.J.J. Leenen, Handboek gezondheidsrecht deel 1: rechten van mensen in de gezondheidszorg, Houten, Bohn Stafleu van Loghum, 2000, pag. 246-247.
[68] Artikel 8 bevat de waarborgen voor betrokkenen zoals: bevoegdheid van kennisname van het bestaan en de doeleinden van het bestand, de identiteit van de houder, de bevoegdheid om in begrijpelijke vorm uitsluitsel te krijgen op de vraag of er persoonsgegevens zijn opgeslagen, de bevoegdheid voor verbetering of wissen van gegevens en de beschikking over rechtsmiddelen als er in strijd met de uitoefening van bovenstaande bevoegdheden wordt gehandeld. Zie F. van der Klaauw-Koops en J. Prins, internationale privacyregulering: belangen, problemen en mogelijkheden, in: J. Prins en J. Berkvens (red.), Privacyregulering in theorie en praktijk, Deventer, Kluwer, 2002, pag.493.
[69] OESO: Organisatie voor Economische Samenwerking en Ontwikkeling; OECD: Organisation for Economic Cooperation and Development.
[70] OECD Recommendation concerning Guidelines Governing the Protection of Privacy and the Transborder Flows of Personal Data, adopted by the Council of the OECD on 23rd September 1980 (OECD privacy Guidelines) OECD Document [C(80)58(Final)], October 1, 1980.

van betrokkenen om kennis te nemen van het feit dat er een geautomatiseerde verwerking met zijn gegevens bestaat, de doeleinden van deze verwerking en de identiteit van de verantwoordelijke[71].

Naast het recht om kennis te nemen van een verwerking maakt ook het recht van toegang tot deze verwerking onderdeel uit van het transparantiebeginsel. Artikel 12 van de privacyrichtlijn geeft betrokkenen het recht om vrijelijk, zonder beperking en zonder bovenmatige vertraging of kosten uitsluitsel te verkrijgen omtrent het bestaan van verwerkingen, de doeleinden van deze verwerking, de (categorieën van) gegevens die verwerkt worden en de ontvangers aan wie deze gegevens worden verstrekt *(individual participation principle)*

De artikelen 18 tot en met 21 van de privacyrichtlijn geven verdere invulling aan het transparantiebeginsel door bepalingen te geven met betrekking tot melding van het voornemen tot verwerking van persoonsgegevens. Artikel 18 geeft de mogelijkheid tot vrijstelling van melding, artikel 19 beschrijft de inhoudseisen waaraan een melding moet voldoen, artikel 20 geeft regels voor meldingen die aan eventueel voorafgaand onderzoek zijn onderworpen en artikel 21 ten slotte geeft opdracht om te zorgen voor openbaarheid van de verwerkingen[72].

In de WBP is het transparantiebeginsel neergelegd in de artikelen 33, 34, 41, 43 en 44. Hoewel in de ICT-privacybeginselen niet expliciet benoemd, maken ook de rechten van betrokkenen deel uit van het transparantiebeginsel; kennisnemen van verwerkingen is onvoldoende indien betrokkenen niet ook de mogelijkheid hebben hun rechten uit te oefenen[73]. Deze rechten zijn het recht op een verzoek tot inzage, correctie, verwijdering, afscherming en verzet. De samenhang met het transparantiebeginsel blijkt mede uit de plaats van deze bepalingen in de WBP. De rechten van betrokkenen zijn opgenomen in de artikelen 5 en 35 tot en met 42; direct aansluitend op de bepalingen aangaande de transparantie[74].

De informatieverstrekking aan betrokkene waarborgt zijn recht te worden geïnformeerd over gegevensverwerking. Dit recht kan door betrokkene op twee manieren worden uitgeoefend: indien de persoonsgegevens rechtstreeks van betrokkene worden verkregen (artikel 33) en wanneer de persoonsgegevens op andere wijze, dus niet rechtstreeks van betrokkene, worden verkregen.

Artikel 33 stelt dat zowel de identiteit van de verantwoordelijke en de doeleinden van de verwerking aan betrokkene moeten worden medegedeeld, vóór het moment van verwerking. Indien de gegevens niet rechtstreeks van betrokkene zijn verkregen dient deze mededeling te geschieden op het moment van vastlegging of op het moment van eerste verwerking indien de gegevens aan een derde zijn verstrekt (artikel 34). Mededeling in dit laatste geval kan slechts achterwege blijven indien betrokkene al op de hoogte is van de verwerking[75], de mededeling onevenredige inspanning kost[76] of de verwerking geschied bij of krachtens wet.
Naast mededeling van verantwoordelijke en doel van de verwerking dient in beide gevallen vastgesteld te worden of betrokkenen nadere informatie moet ontvangen omtrent de verwerking om zo een behoorlijke en zorgvuldige verwerking te waarborgen. De verantwoordelijke kan voor de informatie naar de betrokkene een vergoeding vragen die in specifieke gevallen teruggegeven moet worden.

[71] J. Nouwt, Zorg voor privacy, informatietechnologie en informationele privacy in de gezondheidszorg, Den Haag, SDU, 1997, pag. 338.
[72] J. Nouwt, Zorg voor privacy, informatietechnologie en informationele privacy in de gezondheidszorg, Den Haag, SDU, 1997, pag. 339.
[73] T.F.M. Hooghiemstra, Tekst en toelichting Wet bescherming persoonsgegevens, Koninklijke Vermande, 2003, pag. 23.
[74] G. van Blarkom, J. Leerentveld en R. Schreijnders (red.), Raamwerk privacy audit, Den Haag, CBP, april 2001, pag. 29 en 35.
[75] Deze bepaling is strenger dan de voorganger uit de WPR. Het is echter nog steeds afhankelijk van de omstandigheden of de betrokkene echt op de hoogte is. Slechts bij een beperkt aantal verwerkingen (zoals een ziekenhuisopname) kan worden aangenomen dat de betrokkene op de hoogte is van het feit dat er gegevens worden verwerkt, maar voor de meeste andere verwerkingen zal expliciet informatie over de verwerkingen moeten worden gegeven. H.J.J. Leenen, Handboek gezondheidsrecht deel 1: rechten van mensen in de gezondheidszorg, Houten, Bohn Stafleu van Loghum, 2000, pag. 258.
[76] Een voorbeeld ui de praktijk van het onderzoek: een toekomstig bewoner van een van de locaties van De Vitalis Zorg Groep heeft zich bij de organisatie ingeschreven. Terwijl deze bewoner op wereldreis is, ontvangt Vitalis van diverse instanties (zoals RIO) gegevens over deze betrokkene, gegevens die opgenomen moeten worden in o.m. het cliëntenregistratiesysteem. Volgens artikel 34 zou nu aan de toekomstige bewoner de identiteit van de verantwoordelijke en doelen van de verwerking moeten worden medegedeeld. Deze mededeling is achterwege gebleven omdat het voor de organisatie onevenredige inspanning zou kosten om de betrokkene te traceren.

Criteria af te leiden uit artikel 33, 34 en 39:
1. Zijn de gegevens wel of niet rechtstreeks van betrokkene verkregen?
2. Kan informatie aan betrokkene achterwege blijven en zo ja: waarom?
3. Wanneer is betrokkene op de hoogte gesteld van de verwerking?
4. Welke informatie (doel, identiteit verantwoordelijke en/of aanvullende informatie) heeft betrokkene ontvangen?

Naast de bepalingen omtrent de informatieplicht van de verantwoordelijke vallen ook bepalingen aangaande de rechten van betrokkene, vastgelegd in hoofdstuk 6 WBP, onder het transparantiebeginsel. Deze rechten van betrokkenen zijn te verdelen in: het recht op verzoeken tot inzage, op correctie, op verwijdering, op afscherming en het recht op verzet.

Het recht op verzoek tot inzage is vastgelegd in artikel 35 WBP. Om dit recht te kunnen effectueren moet het voor betrokkene duidelijk zijn waar en hoe een verzoek tot inzage moet worden ingediend en binnen welke termijn op een dergelijk verzoek moet worden gereageerd. In principe moet de verantwoordelijke binnen 4 weken reageren op een dergelijk verzoek. Tevens wordt aangegeven welke informatie deze reactie naar de betrokkene moet bevatten en of een derde, niet zijnde de betrokkene of de verantwoordelijke, de kans moet krijgen bedenkingen tegen de voorgenomen reactie naar betrokkene kenbaar te maken.
Bij verzoeken om inzage kunnen zich bijzondere omstandigheden voordoen. Zo is er de kans dat een belang van de verzoeker dermate zwaar weegt dat een verzoek om informatie op een andere manier dan schriftelijk wordt ingediend. De verantwoordelijke moet in staat zijn ook op deze verzoeken te reageren. Ook bestaat de mogelijkheid dat een verzoek niet door maar namens betrokkenen wordt ingediend indien het gesteld uit artikel 37 WBP van toepassing is. Is de betrokkene jonger dan 16 jaar of onder curatele gesteld, dan moet het verzoek om inzage door de (wettelijk) vertegenwoordiger (bijvoorbeeld een ouder) worden gedaan[77]. Voor invulling van het begrip “wettelijk vertegenwoordiger” kan gebruik gemaakt worden van art 7:465 lid 3 waarin de volgende rangorde voor vertegenwoordigers wordt gegeven:
1. Curator of mentor (ook genoemd de wettelijk vertegenwoordiger),
2. schriftelijk gemachtigde,
3. echtgenoot, geregistreerd partner of andere levensgezel,
4. ouder, kind, broer of zus.

Bij het ontbreken van een wettelijk vertegenwoordiger komt de schriftelijk gemachtigde in aanmerking om de rol van vertegenwoordiger te vervullen mits duidelijk is dat de patiënt/cliënt deze persoon schriftelijk heeft gemachtigd. Op verzoeken van vertegenwoordigers moet de verantwoordelijke reageren alsof het een verzoek van betrokkene betreft, echter de reactie zal ook aan de vertegenwoordiger gericht moeten zijn[78], niet aan betrokkene. Uiteraard is het voor behandeling van alle verzoeken van belang dat de identiteit van verzoeker en/of het vertegenwoordigerschap eenduidig is vastgesteld voordat het verzoek tot inzage wordt behandeld.

Criteria af te leiden uit artikel 35 en 37:
1. Is het voor betrokkene duidelijk hoe en waar een verzoek tot inzage moet worden ingediend?
2. Zijn er termijnen afgesproken voor het geven van een reactie en zo ja, hoe lang zijn deze?
3. Welke gegevens bevat een reactie op een verzoek tot inzage?
4. Hoe kan een derde reageren op de voorgenomen informatieverstrekking naar betrokkene?
5. Hoe is rekening gehouden met de volgende bijzondere omstandigheden:
    a. Verzoek wordt niet schriftelijk ingediend?
    b. Verzoek wordt niet door maar namens betrokkene ingediend?
6. Hoe wordt de identiteit van verzoeker geverifieerd?

Als betrokkene de informatie heeft ontvangen waar hij op grond van artikel 35 recht op heeft, bestaat de kans dat betrokkene concludeert dat de verwerkte gegevens feitelijk onjuist zijn, niet passend zijn bij het doel van de verwerking, onvolledig of juist overmatig zijn dan wel anderszins in strijd met (wettelijke) regels. Betrokkene heeft dan op grond van artikel 36 WBP recht op een verzoek tot verbetering, aanvulling, verwijdering of afscherming van de over hem verwerkte gegevens. Het

[77] L.B. Sauerwein en J.J. Linneman, Handleiding voor verwerkers van persoonsgegevens, Den Haag, Ministerie van Justitie, 2001, pag. 36.
[78] J.M. Witmer, R.P. de Roode (red.), Van wet naar praktijk. Implementatie van de WGBO. Deel 2, KNMG, Utrecht, 2004, pag. 101 e.v.

verzoek moet de aan te brengen wijzigingen bevatten en de verantwoordelijke moet binnen vier weken op het verzoek reageren. De verantwoordelijke kan in principe maar op drie manieren reageren op een verzoek tot wijziging: een met redenen omklede weigering, een uitvoering van de gevraagde wijziging of een mededeling dat de gevraagde wijziging onmogelijk is uit te voeren omdat de gegevensdrager waarop de verwerking is opgeslagen geen wijziging toelaat. De verantwoordelijke heeft op grond van artikel 38 WBP de plicht ook derden aan wie de persoonsgegevens zijn verstrekt van de gevraagde wijziging op de hoogte te stellen, een van de redenen waarom het dus van belang is per verwerking te weten wie ontvangers, gebruikers, derden of verwerkers zijn. Ook voor het behandelen van wijzigingsverzoeken gelden de acties bij bijzondere omstandigheden uit artikel 37 WBP.
Vallen de verwerkte persoonsgegevens onder de medische gegevens en zijn ze opgenomen in een medisch dossier[79] zoals bedoeld in artikel 7:454 BW dan ontstaan er verschillen met de WBP. Betrokkene i.c. de patiënt heeft te allen tijde inzage in de gegevens in het dossier en een hulpverlener moet aan een dergelijk verzoek zo spoedig mogelijk (ex artikel 7:456 BW) maar in ieder geval binnen 4 weken (ex artikel 35 WBP) voldoen, analoog aan het gestelde in artikel 35 WBP. Hierop is slechts één uitzondering mogelijk[80]: wanneer de persoonlijke levenssfeer van een ander dan de patiënt door de inzage kan worden geschaad, waarbij het belang van deze derde een overwegend karakter dient te hebben ten opzichte van het belang van de betrokkene. Waar onder het gestelde van artikel 36 WBP een verantwoordelijke nog een verzoek tot aanvulling of verbetering van de verwerkte persoonsgegevens mag weigeren, is dit onder artikel 7:454 lid 2 niet toegestaan voor verzoeken tot aanvulling of verbetering van het medisch dossier[81].
Op het eerste gezicht lijkt het alsof de WGBO de patiënt via artikel 7:455 BW een recht op vernietiging van de in het dossier bewaarde medische bescheiden toekent, maar lid 2 van dit artikel geeft de hulpverlener een mogelijkheid tot uitzondering op dit recht, waardoor de praktijk weinig zal verschillen van de variaties die door artikel 36 WBP mogelijk worden gemaakt (weigering, uitvoering of onmogelijkheid tot verwijderen).

Criteria af te leiden uit artikel 35, 36, 37 en 38

1. Is het voor betrokkene duidelijk hoe en waar een verzoek tot wijziging moet worden ingediend?
2. Zijn er termijnen afgesproken voor het geven van een reactie en zo ja, hoe lang zijn deze?
3. Is het duidelijk dat een verzoek tot wijziging slechts op drie manieren beantwoordt mag worden?
4. Hoe worden wijzigingen doorgegeven aan derden?
5. Hoe is rekening gehouden met de volgende bijzondere omstandigheden:
    a. Verzoek wordt niet schriftelijk ingediend?
    b. Verzoek wordt niet door maar namens betrokkene ingediend?
6. Hoe wordt de identiteit van verzoeker geverifieerd?

Naast de rechten uit artikel 36 heeft betrokkene op grond van artikel 40 en 41 ook het recht bezwaar aan te tekenen tegen verwerking van zijn persoonsgegevens: het recht van verzet. Dit recht van verzet bestaat in een relatieve vorm en een absolute vorm. Indien de verantwoordelijke gegevens verwerkt op de grondslag van artikel 8 sub e of sub f kan betrokkene “relatief” verzet aantekenen in verband met bijzondere persoonlijke omstandigheden waarbij het aan betrokkene is om te stellen en te bewijzen dat er sprake is van bijzondere persoonlijke omstandigheden. Op dit verzoek moet binnen 4 weken worden gereageerd en indien het verzet gerechtvaardigd is dient de verwerking te worden stopgezet.

[79] Slechts de persoonlijke werkaantekeningen van de hulpverlener vallen niet onder het dossier waarbij het moet gaan om apart opgeborgen en niet voor anderen toegankelijke aantekeningen die de hulpverlener voor persoonlijk gebruik nodig heeft. Deze moeten ook direct na de behandeling worden vernietigd. Zo gauw aantekeningen in het dossier worden gevoegd en/of voor anderen toegankelijk zijn, vallen ze onder het inzagerecht en de overige plichten m.b.t. het zorgdossier. H.J.J. Leenen, Handboek gezondheidsrecht deel 1: rechten van mensen in de gezondheidszorg, Houten, Bohn Stafleu van Loghum, 2000, pag. 260.
[80] Niet te verwarren met de therapeutische exceptie waarbij de behandelaar kan besluiten informatie niet te verstrekken aan de patiënt. Dit is volgens de WGBO slechts toegestaan als het wel verstrekken van informatie ernstig nadeel voor de patiënt kan opleveren (art 7:448 lid 3 BW). Ook al kan inzage kennis opleveren voor de patiënt die door de hulpverlener vanwege de therapeutische exceptie nog niet was medegedeeld, dan is dit nog geen grond voor het introduceren van de therapeutische exceptie in het inzagerecht. Het inzagerecht speelt tussen de verantwoordelijke en de betrokkene, de therapeutische exceptie tussen de hulpverlener en de betrokkene. H.J.J. Leenen, Handboek gezondheidsrecht deel 1: rechten van mensen in de gezondheidszorg, Houten, Bohn Stafleu van Loghum, 2000, pag. 260.
[81] J. Nouwt, Privacy en medische informatie in: J. Prins en J. Berkvens (red.), Privacyregulering in theorie en praktijk, Kluwer, Deventer, 2002, pag. 265.

Indien de verwerking geschied met het oog op commerciële of charitatieve bedoelingen[82] heeft de betrokkene het recht op absoluut verzet. Dit wil zeggen dat de verwerking wordt vermoed inbreuk te maken op bijzondere omstandigheden en dat de verantwoordelijke direct de verwerking moet stoppen. De verantwoordelijke voor dit type van verwerking heeft de plicht de betrokkenen te wijzen op de mogelijkheid van absoluut verzet.

Criteria af te leiden uit artikel 40 en 41:
1. Is het voor betrokkene duidelijk hoe en waar een verzet moet worden ingediend?
2. Is betrokkene gewezen op de mogelijkheid van absoluut verzet?
3. Zijn er termijnen afgesproken voor het geven van een reactie en zo ja, hoe lang zijn deze?
4. Zijn er maatregelen getroffen om de verwerking terstond (bij absoluut verzet) dan wel na gerechtvaardigd relatief verzet, te beëindigen?

Vanuit het gestelde in art 42 WBP ontlenen betrokkenen het recht niet onderworpen te worden aan een besluit [..] indien dat besluit alleen genomen wordt op grond van een geautomatiseerde gegevensverwerking [..]. Een dergelijk besluit kan wél worden genomen indien het wordt genomen in het kader van het sluiten of uitvoeren van een overeenkomst en er passende maatregelen zijn genomen ter bescherming van gerechtvaardigde belangen van betrokkene. Ook mag een geautomatiseerd besluit worden genomen indien dit gebeurt op basis van een wettelijke grondslag en er in deze wet maatregelen zijn vastgelegd die eveneens strekken tot bescherming van de gerechtvaardigde belangen van betrokkene[83].

Criteria af te leiden uit artikel 42:
1. Worden er besluiten genomen die zijn gebaseerd op geautomatiseerde verwerking?
2. Binnen welk kader zijn deze besluiten genomen?
3. Is er een wettelijke grondslag die een geautomatiseerd besluit toestaat?

6.3 Doelbinding

Dit beginsel stelt dat gegevens alleen maar mogen worden verwerkt onder vooraf uitdrukkelijk omschreven en gerechtvaardigde doeleinden *(purpose specification principle)*. Hieronder valt ook de beperking op de hoeveelheid gegevens; niet meer gegevens mogen worden verzameld en verwerkt dan noodzakelijk voor het behalen van deze doelen. De verzamelde gegevens mogen daarnaast niet worden gebruikt voor doeleinden die niet met het oorspronkelijke doel verenigbaar zijn (*use limitation principle).*

De WBP codificeert doelbinding in artikel 7 en 9[84]. In paragraaf 5.2.4 is de achtergrond van dit beginsel als onderdeel van de inventarisatie van bestaande verwerkingen al aan de orde geweest. In artikel 7 WBP wordt gesteld dat verwerking slechts mag plaatsvinden voor welomschreven en vooraf bepaalde doelen. Dit impliceert dat het doel zoals dat tijdens de inventarisatie dient te worden vermeld voldoende concreet en duidelijk moet zijn weergegeven. Een te abstracte omschrijving van het doel is geen middel om de eis van verenigbaarheid van doel te omzeilen omdat hiermee de doelbeschrijving niet in overeenstemming is met de eis van concrete en duidelijke formulering[85].
Artikel 9 is een aanvulling op dit doelvereiste namelijk dat gegevens alleen mogen worden verwerkt voor zover zij verenigbaar zijn met het genoemde doel. De ingrijpendheid van de gevolgen van de verwerking voor betrokkene is de factor die van belang is bij de toets op verenigbaarheid[86]. Deze verenigbaarheid wordt getoetst aan de hand van de verwantschap tussen het doel van de beoogde verwerking en het oorspronkelijk doel, de aard van de gegevens en de wijze waarop ze zijn verkregen, de gevolgen van de beoogde verwerking voor betrokkene en de mate waarin wordt voorzien in

[82] Hoewel dit in eerste instantie niet lijkt aan te sluiten bij de kernactiviteiten van een zorginstelling, komen deze activiteiten in de praktijk toch voor o.a. in de vorm van informatiemailings naar mensen die interesse hebben getoond in Vitalis, sponsoractiviteiten etc.
[83] J. Prins en J. Berkvens, De Wet bescherming persoonsgegevens in: J. Prins en J. Berkvens (red.), Privacyregulering in theorie en praktijk, Deventer, Kluwer, 2002, pag. 95.
[84] G. van Blarkom, J. Leerentveld en R. Schreijnders (red.), Raamwerk privacy audit, Den Haag, CBP, april 2001, pag. 31. In deze publicatie wordt ook artikel 10 WBP onder “doelbinding” meegenomen terwijl in dit verslag de bepalingen aangaande bewaartermijnen uit artikel 10 worden behandeld in paragraaf 6.7.
[85] T.F.M. Hooghiemstra, Tekst en toelichting Wet bescherming persoonsgegevens, Koninklijke Vermande, 2003, pag. 62.
[86] T.F.M. Hooghiemstra, Tekst en toelichting Wet bescherming persoonsgegevens, Koninklijke Vermande, 2003, pag. 24.

passende waarborgen jegens betrokkene. Zoals reeds in paragraaf 5.2.4 geconcludeerd zullen deze criteria feitelijk moeten worden ingevuld.

In het Vrijstellingsbesluit zijn, per verwerking, de toegestane doelen opgenomen. Het Vrijstellingsbesluit kan voor vrijgestelde (of niet-gemelde) verwerkingen de toetssteen vormen voor het bepalen of het doel van een voorgenomen verwerking in overeenstemming is met het doel waarvoor de gegevens oorspronkelijk werden verwerkt. Indien zowel het oorspronkelijke doel als het beoogde doel beiden in dezelfde lijst voorkomen, is dit een eerste indicatie dat de voorgenomen verwerking zal gaan voldoen aan de eis van doelbinding.
Eenzelfde redenering gaat op voor de aard van de gegevens. Ook hier biedt het Vrijstellingsbesluit overzichten van typen gegevens die verwerkt mogen worden. Als de reeds verwerkte gegevens ook zijn benoemd als toelaatbaar onder het beoogde doel, is dit een tweede aanwijzing dat de beoogde verwerking hoogstwaarschijnlijk voldoet aan de doelbindingseis.
Bij het vaststellen van de gevolgen van de beoogde verwerking kan ook gebruik gemaakt worden van de criteria van het vrijstellingsbesluit. De essentie van dit besluit, zoals opgenomen in artikel 29 WBP, stelt in feite dat het voor vrijgestelde verwerkingen onwaarschijnlijk is dat zij inbreuk maken op de fundamentele vrijheden van betrokkene.
Indien zowel het oorspronkelijke doel als het beoogde doel beiden voorkomen in het Vrijstellingsbesluit en de aard van de verwerkte gegevens hetzelfde is, kan hieruit dus worden afgeleid dat de gevolgen van beide verwerkingen in beginsel geen inbreuk maken op de fundamentele vrijheden van de betrokkene.

Een voorbeeld: een sollicitant biedt zijn CV aan. De gegevens over genoten opleidingen hieruit worden primair gebruikt om te beoordelen of de sollicitant geschikt is voor de functie (het oorspronkelijke doel). De gegevens over de woonplaats van de sollicitant worden daarna gebruikt om de hoogte van de reiskostenvergoeding vast te stellen (het beoogde doel). Volgens artikel 5 van het Vrijstellingsbesluit vallen het oorspronkelijke doel en het beoogde doel beiden onder de toegestane verwerkingen van lid 2. Er is dus een duidelijke verwantschap tussen de doelen.
De verwerkte gegevens zijn onder het oorspronkelijke doel beperkt tot de opleiding en ervaring van de sollicitant en in het tweede geval tot adres en woonplaats. Beide typen worden genoemd in lid 3 van artikel 5 en kunnen dus tot dezelfde categorie worden gerekend. Ook hier is er dus verwantschap.
Beide typen gegevens zijn daarnaast rechtstreeks van betrokkene verkregen.
Rest in dit voorbeeld nog de toets op de gevolgen voor de betrokkenen van de oorspronkelijke verwerking (beoordeling van de geschiktheid) en de voorgenomen verwerking (de reiskostenvergoeding). Beide verwerkingen zijn benoemd in het Vrijstellingsbesluit en dus kan er, gezien het gestelde in artikel 29 WBP, vanuit worden gegaan dat er in dit geval geen inbreuk is op de fundamentele vrijheden van betrokkene.
In dit voorbeeld zal de conclusie dus zijn dat ook de beoogde verwerking voldoet aan de eis van doelbinding.
Binnen de praktijk van een zorginstelling als Vitalis zal het doel van de verwerking van personalia van medewerkers meestal identificatie en communicatie zijn. Het doel van verwerking van administratieve en financiële gegevens van medewerkers is administratie, financiering, pensioenaanspraken en uitvoering geven aan bepalingen uit sociale en fiscale wetgeving. Het doel van verwerking van bewoners- en cliëntgegevens is meestal goed hulpverlenerschap, identificatie en communicatie, administratie en financiering van de zorg, kwaliteitszorg en uitvoering klachtenrecht en voor sommige gegevens de uitvoering van een wettelijke plicht.

Criteria af te leiden uit artikel 7 en 9:

1. Is er een verschil tussen het doel waarvoor de gegevens zijn verkregen en het doel waarvoor ze worden verwerkt? Hierbij kan gebruik gemaakt worden van de benoemde “zorgproducten” en de differentiatie in “personeelsdiensten” uit paragraaf 5.3 en de concretisering hiervan in het Vrijstellingsbesluit
2. Welk type gegevens wordt verwerkt, vallen de verwerkte gegevens in dezelfde categorie? Hier kan de beschrijving uit paragraaf 5.2.6 ondersteunend zijn in combinatie met de opsommingen van gegevens die worden gebruikt in het Vrijstellingsbesluit.
3. Van wie zijn de gegevens verkregen?
4. Wat zijn de gevolgen voor betrokkene waarbij het wel / niet benoemd zijn in het Vrijstellingsbesluit een aanwijzing is?

6.4 Rechtmatige grondslag voor verwerking

Naast een concreet en duidelijk omschreven doel voor de verwerking vraagt de WBP ook een rechtmatige grondslag voor de verwerking. Persoonsgegevens mogen alleen worden verzameld en verwerkt wanneer de grondslag hiervoor in de WBP kan worden gevonden. De WBP geeft een zestal grondslagen voor verwerking waarvan er minimaal één van toepassing moet zijn; elke gegevensverwerking of categorie van verwerkingen dient herleidbaar te zijn tot een van de in artikel 8 limitatief benoemde grondslagen[87]. Voor bijzondere persoonsgegevens gelden zelfs nog aanvullende, specifieke regels, gebaseerd op het uitgangspunt dat bijzondere persoonsgegevens niet mogen worden verwerkt tenzij daarvoor een wettelijke mogelijkheid is gegeven. Criteria voor de beoordeling van de rechtmatigheid van verwerking zijn in de WBP opgenomen in de artikelen 6, 8 en 16 tot en met 23[88].
In paragraaf 5.2.4 is al een beschrijving gegeven van het rechtmatigheidsbeginsel, de criteria waarop getoetst kan worden kunnen nu uit de WBP worden afgeleid.

Als eerste grondslag is er de ondubbelzinnige toestemming van betrokkenen voor de verwerking. Hiermee wordt de beschikkingsmacht die een betrokkene heeft over de verwerking van zijn gegevens expliciet gemaakt[89]. Er zijn echter ook gevallen waarin de wet de toestemming van betrokkenen als rechtmatige grondslag voor verwerking uitsluit zoals in situaties waarin sprake is van ongelijke verhouding tussen verantwoordelijke en betrokkene. Een voorbeeld hiervan was te vinden in artikel 4 van de Wet SAMEN en artikel 5 Wet op de medische keuringen. Ook de WBP zelf ziet toestemming van betrokkene niet als voldoende rechtvaardigingsgrond in de artikelen 17 lid 3, 18, 19 lid 2, 20 lid 2 en 21 lid 4[90]. Het criterium voor controle van toestemming is dat van ondubbelzinnigheid; bij de verantwoordelijke dient elke twijfel over het al dan niet verlenen van toestemming door betrokkene te zijn uitgesloten. Indien er sprake is van het vereiste van uitdrukkelijke toestemming, dient deze gegeven te zijn middels een expliciete wilsuiting in woord, geschrift of gedrag.

Criteria
1. Is voor deze verwerking de toestemming van betrokkenen een voldoende grondslag?
2. Is de verleende toestemming ondubbelzinnig?

In onderdeel b van artikel 8 wordt de (pre)contractuele verplichting als gerechtvaardigde grondslag van verwerking toegestaan. Eerste voorwaarde hierbij is dat betrokkene zelf of via een vertegenwoordiger partij is bij de overeenkomst. Als dit onderdeel van artikel 8 wordt gebruik dient dus getoetst te worden op de aanwezigheid van een (pre)contractuele relatie waarbij betrokkene partij is. In de precontractuele fase moet het gaan om handelingen die op verzoek van betrokkene zijn verricht om een overeenkomst te kunnen sluiten, waarbij de verwerkingshandelingen logisch moeten voortvloeien uit het verzoek en het ook voor betrokkene duidelijk is dat deze handelingen (moeten) worden verricht[91]. Binnen de gezondheidszorg wordt de Wet geneeskundige behandelingsovereenkomst (WGBO) gezien als een overeenkomst die verwerking van persoonsgegevens toestaat[92].

Criteria
1. Is er sprake van een (pre)contractuele verplichting?
2. Is betrokkene partij in deze overeenkomst?
3. Is er een verzoek van betrokkene indien sprake is van een precontractuele fase?
4. Is verwerking noodzakelijk voor nakoming van de (pre)contractuele verplichtingen?

---

[87] T.F.M. Hooghiemstra, Tekst en toelichting Wet bescherming persoonsgegevens, Den Haag, Koninklijke Vermande, 2003, pag. 24.
[88] G. van Blarkom, J. Leerentveld en R. Schreijnders (red.), Raamwerk privacy audit, Den Haag, CBP, april 2001, pag. 33 en T.F.M. Hooghiemstra, Tekst en toelichting Wet bescherming persoonsgegevens, Den Haag, Koninklijke Vermande, 2003, pag. 24.
[89] J.G. Brouwer, Compendium Wet bescherming persoonsgegevens, tekst en toelichting, Den Haag, Koninklijke Vermande, 2002, pag. 106.
[90] J.G. Brouwer, Compendium Wet bescherming persoonsgegevens, tekst en toelichting, Den Haag, Koninklijke Vermande, 2002, pag. 107.
[91] J.G. Brouwer, Compendium Wet bescherming persoonsgegevens, tekst en toelichting, Den Haag, Koninklijke Vermande, 2002, pag. 107 en T.F.M. Hooghiemstra, Tekst en toelichting Wet bescherming persoonsgegevens, Den Haag, Koninklijke Vermande, 2003, pag. 63.
[92] T.F.M. Hooghiemstra, Privacy bij ICT in de Zorg. Bescherming van persoonsgegevens in de informatiestructuur van de gezondheidszorg, Den Haag, CBP, 2002, pag. 36.

Het derde onderdeel van artikel 8, onderdeel c, geeft toestemming voor verwerking indien deze nodig is om aan een wettelijke verplichting, waaraan de verantwoordelijke is onderworpen, te voldoen. Deze formulering bevat de twee toetsingscriteria: de verantwoordelijke dient te zijn belast met de uitvoering van een wettelijke verplichting en de gegevensverwerking moet noodzakelijk zijn ter uitvoering van deze verplichting. Aandachtspunt hierbij is dat deze wettelijke verplichting niet de expliciete opdracht tot gegevensverwerking behoeft te bevatten.
Het moet bij toepassing van deze grondslag gaan om een verplichting waaraan de verantwoordelijke zelf is onderworpen; wettelijke verplichtingen van derden vallen onder onderdeel f van artikel 8. Voor wat betreft het noodzakelijkheidscriterium moet worden gesteld dat nakoming van de wettelijke verplichting niet mogelijk is zonder verwerking. Het begrip wettelijke verplichting omvat alle verplichtingen tot gegevensverwerking die krachtens algemeen verbindend voorschrift worden opgelegd[93], waarbij echter steeds moet worden voldaan aan de beperkingssystematiek uit artikel 10 GW[94]. Een voorbeeld van de verplichting tot verwerking is o.m. te vinden in hoofdstuk 2 van de Infectieziektenwet[95] of de registerbepalingen uit de wet BIG.

Criteria
1. Welke wettelijke verplichting is de grondslag voor verwerking?
2. Is het redelijkerwijs onmogelijk om aan genoemde verplichting te voldoen zonder deze verwerking?

Het “vitale belang” zoals genoemd in onderdeel d van artikel 8 dient eng te worden geïnterpreteerd. Er moet sprake zijn van een dringende medische noodzaak om gegevens van betrokkene te verwerken. Ernstig gevaar voor de volksgezondheid is onvoldoende, er dient uitgegaan te worden van een zaak van leven of dood voor betrokkene (vitaal in de zin van levensbedreigend)[96]. Deze grondslag mag slechts worden gebruikt indien het in redelijkheid niet mogelijk is toestemming van betrokkene te vragen in de zin van onderdeel a van artikel 8.

Criterium
1. Werd de mogelijkheid om toestemming te vragen uitgesloten door een, voor betrokkene, levensbedreigende omstandigheid?
2. Is er sprake van voldoende (medische) noodzaak tot verwerking?

De tot nu toe gegeven grondslagen zijn specifiek omdat er telkens op een duidelijk omschreven doel kon worden getoetst. Onderdeel f van artikel 8 is een flexibele toevoeging omdat het in de praktijk onmogelijk is een sluitende regeling van wettelijk toegestane grondlagen te vormen[97]. De Richtlijn geeft middels overweging 30 (“het dagelijks beheer van ondernemingen en andere organisaties”) een indicatie welke belangen onder dit onderdeel als rechtvaardig kunnen worden beschouwd. De wet verbiedt het verwerken van gegevens die voor het behoorlijk functioneren van een organisatie noodzakelijk zijn dus niet, mits voldoende rekening is gehouden met de belangen van betrokkenen. Dit zelfde is van toepassing op verwerkingen die niet direct deel uitmaken van het primaire proces van de verantwoordelijke maar hieraan wel direct ondersteunend zijn. De toets op noodzakelijkheid van verwerkingen die op deze grondslag worden uitgevoerd bestaat uit een aantal vragen.

Criteria
1. Is het belang van verantwoordelijke werkelijk gerechtvaardigd?
2. Wordt er met de verwerking een inbreuk gemaakt op de rechten van betrokkene?
3. Kan het doel dat met de verwerking wordt beoogd ook langs andere weg worden bereikt?
4. Is de verwerking proportioneel aan het nagestreefde doel?

[93] Waarbij ook communautair en internationaal recht een dergelijke verplichting kunnen opleggen. Zie J.G. Brouwer, Compendium Wet bescherming persoonsgegevens, tekst en toelichting, Den Haag, Koninklijke Vermande, 2002, pag. 108.
[94] Een verplichting kan alleen bij of krachtens een wet in formele zin in het leven worden geroepen.
[95] Wet van 11 juni 1998, houdende regels ter afwending van de gevaren van infectieziekten.
[96] J.G. Brouwer, Compendium Wet bescherming persoonsgegevens, tekst en toelichting, Den Haag, Koninklijke Vermande, 2002, pag. 109 en T.F.M. Hooghiemstra, Tekst en toelichting Wet bescherming persoonsgegevens, Den Haag, Koninklijke Vermande, 2003, pag. 64.
[97] J.G. Brouwer, Compendium Wet bescherming persoonsgegevens, tekst en toelichting, Den Haag, Koninklijke Vermande, 2002, pag. 110 en T.F.M. Hooghiemstra, Tekst en toelichting Wet bescherming persoonsgegevens, Den Haag, Koninklijke Vermande, 2003, pag. 64.

Binnen Vitalis zal de grondslag voor het verwerken van persoongegevens van medewerkers meestal zijn artikel 7:610 BW (de arbeidsovereenkomst). Daarnaast is er vaak een wettelijke verplichting tot verwerking, met name binnen de sociale wetgeving (b.v. art. 8 Wet REA, AWR, AOW, Poortwachter). Bij vrijwillige deelname aan activiteiten zoals een personeelsvereniging is de grondslag gelegen in de toestemming tot verwerking van de betrokkene. Verwerkingen die te maken hebben met gebruik van het netwerk, toegangscontrolesystemen, videobewaking van complexen e.d. zijn terug te voeren op onderdeel f van artikel 8 WBP.
Bij verwerking van gegevens van bewoners en cliënten zal, juist binnen een zorginstelling als Vitalis, artikel 7:446 (de geneeskundige behandelingsovereenkomst) de grondslag zijn zoals bedoeld in artikel 8 onder b WBP (overeenkomst). Ook huur-, koop- of leveringsovereenkomsten zijn regelmatig voorkomende grondslagen voor verwerking. Wetgeving die een zorginstelling de plicht tot registratie oplegt is o.m. de KWZ (art. 3, 4), AWBZ (art. 8g, 56), WKCZ (art. 2)[98] of de Infectieziektenwet.

6.5 Kwaliteit van de gegevens

Het kwaliteitsbeginsel valt in twee onderdelen uiteen: de verzamelde persoonsgegevens moeten relevant zijn voor het doel waarvoor zij worden verwerkt ofwel de gegevens moeten toereikend, ter zake dienend en niet overmatig zijn in relatie tot het doel waarvoor ze worden verwerkt *(collection limitation principle)*. Daarnaast moeten de persoonsgegevens juist, accuraat, volledig en actueel zijn *(data quality principle)*. Dit impliceert mede dat ze, indien nodig, worden bijgewerkt en dat er redelijke maatregelen zijn getroffen om onjuistheden en tekortkomingen te herstellen. De WBP waarborgt de kwaliteit van de gegevens vanuit het gestelde in de artikelen 6 en 11[99].

De kwaliteitseis uit artikel 11 lid 1 valt uiteen in de reeds genoemde drie elementen: niet bovenmatig, toereikend en ter zake dienend. Niet bovenmatig betekent dat de verwerkte gegevens niet meer details mogen bevatten dan voor het bereiken van het oorspronkelijke (en vooraf vastgelegde) doel noodzakelijk is. Hiertegenover staat de eis dat de verwerking voldoende gegevens moet bevatten om tot een volledig beeld van de betrokkene binnen de doelstelling te komen; ontoereikende verwerking zal er immers toe leiden dat het gestelde doel niet wordt behaald[100]. Het derde element, ter zake dienend, lijkt op de eerste eis maar heeft betrekking op het al of niet overbodig zijn van gegevens. Lid 2 legt de verantwoordelijke de verplichting op maatregelen te treffen om te controleren of de verwerkte gegevens juist en volledig zijn. Het gaat hier dus niet om de absolute verplichting te allen tijde na te gaan of de verwerkte gegevens juist zijn, maar om het verwezenlijken van controlesystemen om op periodieke basis de juistheid van gegevens te controleren[101]. De volgende toetsingscriteria zijn uit deze eisen af te leiden:

Criteria
1. Worden de gegevens zo dicht mogelijk bij de bron gevalideerd, gecontroleerd en verwerkt?
2. Is er een controle op de relatie tussen verwerkte gegevens en beoogd doel voor wat betreft hoeveelheid verwerkte gegevens?
3. Is er een controlemechanisme op juistheid van de gebruikte gegevens bij invoer, verwerking en uitvoer?
4. Is er een controlemechanisme voor de controle op actualiteit van de verwerkte gegevens?
5. Zijn er maatregelen genomen om het moment van ontstaan van onjuistheden te achterhalen?
6. Zijn er maatregelen getroffen om geconstateerde onjuistheden te verbeteren?

6.6 Beveiliging van gegevens

6.6.1 Inleiding

De essentie hier is dat de verantwoordelijke ervoor zorg draagt dat alle passende technische en organisatorische maatregelen worden getroffen om verlies, beschadiging of onrechtmatige verwerking

[98] Kwaliteitswet Zorginstellingen, Wet Klachtenrecht Cliënten Zorginstellingen, Algemene wet bijzondere ziektekosten.
[99] G. van Blarkom, J. Leerentveld en R. Schreijnders (red.), Raamwerk privacy audit, Den Haag, CBP, april 2001, pag. 34.
[100] L.B. Sauerwein en J.J. Linneman, Handleiding voor verwerkers van persoonsgegevens, Den Haag, Ministerie van Justitie, 2001, pag. 28.
[101] L.B. Sauerwein en J.J. Linneman, Handleiding voor verwerkers van persoonsgegevens, Den Haag, Ministerie van Justitie, 2001, pag. 29.

van gegevens te voorkomen *(security safeguards principle).* Ook moeten er zo min mogelijk gegevens worden gebruikt die herleidbaar zijn tot individuele personen. De artikelen 6, 12 en 13 WBP vormen samen de basis voor de beveiligingsmaatregelen door de verantwoordelijke. Artikel 14 WBP legt de eis van beveiliging ook neer bij de bewerker. De maatregelen ter beveiliging kunnen in drie soorten worden onderscheiden[102].

Allereerst is er de geheimhoudingsplicht uit artikel 12. Degenen die persoonsgegevens verwerken moeten hiertoe, van de verantwoordelijke, de bevoegdheid hebben gekregen. Ook hebben deze medewerkers een geheimhoudingsplicht over de gegevens waar zij toegang tot hebben. Dit impliceert dat ook medewerkers voor wie niet een expliciete geheimhouding op grond van ambt, beroep of wettelijk voorschrift van toepassing is, alsnog op grond van artikel 12 lid 2 tot geheimhouding verplicht zijn van de persoonsgegevens waarvan zij kennis nemen. In de Nederlandse regelgeving is het wettelijke beroepsgeheim voor medisch beroepsbeoefenaars o.m. terug te vinden in artikel 21 Wet Verkrijging bevoegdheid arts, tandarts, apotheker, vroedvrouw en apothekersbediende, in artikel 7 van de Wet op de paramedische beroepen, en in artikel 88 Wet Beroepen in de individuele gezondheidszorg (BIG). Via het gestelde in de WGBO is expliciet het reeds geldende recht met betrekking tot geheimhouding van medische gegevens wettelijk vastgelegd. Dit geldende recht houdt, kort gezegd, in dat de plicht tot geheimhouding die op een hulpverlener rust slecht met toestemming van de patiënt zelf kan worden opgeheven, behoudens enkele bij of krachtens wet[103] geregelde gevallen[104].

De tweede beveiligingseis is artikel 13: het nemen van passende technische en organisatorische maatregelen tegen verlies en onrechtmatige verwerking. Deze ruime formulering vraagt om nadere invulling, met name het begrip passend. Bij het invullen van deze maatregelen dient de verwerkende organisatie of instelling bij de keuze voor maatregelen een aantal elementen in de beoordeling mee te nemen. Ten eerste is daar de beoordeling van de aard van de te verwerken gegevens; hoe gevoeliger de gegevens, des te zwaarder de eisen die aan de beveiliging moeten worden gesteld. Ook moet de instelling de afweging maken tussen de stand van de techniek en de kosten van extra maatregelen. Als de kosten van additionele beveiligingsmaatregelen extreem hoog zijn ten opzichte van de toename in beveiliging, dan zijn de maatregelen niet passend en hoeven deze ook niet toegepast te worden. Bestaat echter de mogelijkheid om met relatief geringe investeringen een duidelijk veiligere verwerking te realiseren, dan moeten deze maatregelen inderdaad verwezenlijkt worden[105]. De beveiliging die een organisatie heeft, dient steeds voldoende te zijn. Hierdoor ontstaat voor de organisatie de verplichting om continu te toetsen of de bestaande maatregelen in combinatie met de stand van de techniek en de organisatie voldoende zijn of aanpassing behoeven en onderling samenhangend zijn.

De technische maatregelen die een organisatie kan nemen omvatten de logische en fysieke maatregelen in en rond de informatiesystemen zoals toegangscontrole en autorisatie, vastlegging van gebruik en back-up[106]. Privacy Enhancing Technologies (PET[107]) kunnen ook een belangrijk hulpmiddel zijn om aan de technische eisen van artikel 13 te voldoen. Naast een technische component omvat beveiliging ook organisatorische maatregelen voor de inrichting van de verwerkende organisatie en de verwerking zelf, zoals toekenning en deling van verantwoordelijkheden en bevoegdheden, trainingen en calamiteiten- en uitwijkplannen. Indien er voor de beveiliging de keuze is tussen een technische en een organisatorische maatregel verdient de technische maatregel

[102] J. Nouwt, Invoering van de WBP in tien stappen, http://rechten.uvt.nl/sjaaknouwt/Zorgvisi.doc , pag. 3 en WBP, Handleiding bij het invoeren van de wet bescherming persoonsgegevens, VOG, Utrecht, 2001, pag. 14-15.
[103] Bijvoorbeeld het inzagerecht van de (hoofd)inspecteurs in de dossiers van patiënten die zijn opgenomen onder de Wet BOPZ zoals gegeven door artikel 63 lid 4 van deze wet.
[104] J. Nouwt, Privacy en medische informatie in: J. Prins en J. Berkvens (red.), Privacyregulering in theorie en praktijk, Kluwer, Deventer, 2002, pag. 256.
[105] WBP, Handleiding bij het invoeren van de wet bescherming persoonsgegevens, VOG, Utrecht, 2001, pag. 15.
[106] G.W. van Blarkom, J.J. Borking, Beveiliging van persoonsgegevens, Registratiekamer, Den Haag, 2001, pag. 15.
[107] PET wordt gedefinieerd als een samenhangend geheel van maatregelen dat de persoonlijke levenssfeer beschermt door het elimineren of verminderen van persoonsgegevens of door het voorkomen van onnodige dan wel ongewenste verwerking van persoonsgegevens, een en ander zonder verlies van de functionaliteit van het informatiesysteem. S.M. Artz en L.E. van Laviere, De Wet bescherming persoonsgegevens, over de bescherming van uw persoonlijke gegevens, Den Haag, CBP, 2002, pag. 17.

de voorkeur. De ratio van deze voorkeur is het feit dat het moeilijker is om aan het effect van technische maatregelen te ontkomen waardoor deze maatregelen doeltreffender zijn[108].

De derde eis met betrekking tot beveiliging van persoonsgegevens richt zich op de deugdelijkheid van de beveiligingsmaatregelen die een bewerker neemt bij het verwerken van persoonsgegevens in opdracht van de verantwoordelijke. De verantwoordelijke heeft de plicht om in zijn overeenkomst met de bewerker deze voldoende duidelijk te maken hoe met de te verwerken persoonsgegevens moet worden omgegaan. De verantwoordelijke dient ook toe te zien op de feitelijke naleving van deze verplichtingen

Voor elke afzonderlijke verwerking van persoonsgegevens zal dus vastgesteld moeten worden welke technische en organisatorische maatregelen zijn genomen en of deze afdoende zijn om het gewenste passende niveau van beveiliging te bereiken. Er kan geen algemeen oordeel gegeven worden over wat als passend kan worden beschouwd; het begrip passend duidt er op dat de maatregelen per geval in overeenstemming dienen te zijn met de risico's die de betrokken verwerking en de aard van de te beschermen gegevens met zich meebrengen[109]. Om te komen tot concrete normen voor beveiliging waarop de organisatie getoetst kan worden zal eerst een risicoverdeling moeten worden gemaakt waarmee de te beoordelen verwerkingen in een klasse kunnen worden ingedeeld. Per klasse kan dan een norm worden gedefinieerd waaraan de beveiliging van deze klasse moet voldoen. Tot slot zal deze norm vertaald moeten worden naar een aantal concrete eisen op de deelgebieden van informatiebeveiliging.

Voor het vaststellen van de risicoklassen is aansluiting gezocht bij het model dat door het CBP gebruikt wordt in AV23[110]. In dit model wordt uitgegaan van vier risicoklassen.

Risicoklasse 0: publiek niveau
In deze categorie vallen de openbare persoonsgegevens waarbij het algemeen aanvaard is dat deze, bij beoogd gebruik en binnen de overige eisen van de wet zoals doelbinding, geen risico opleveren voor de betrokkene. De verwerkingen die betrekking hebben op deze gegevens hoeven niet beter beveiligd te worden dan noodzakelijk om een voldoende kwaliteit van informatie tot stand te brengen en in stand te houden. De WBP stelt voor beveiliging van deze gegevens dus geen additionele eisen onder artikel 13 en het CBP geeft dan ook aan dat voor deze risicoklasse geen specifieke maatregelen hoeven te worden genomen. Criterium om in deze categorie te vallen is dus dat de verwerkte gegevens (toch al) openbaar beschikbaar zijn.

Risicoklasse I: basisniveau
Binnen deze klasse zijn standaard beveiligingsmaatregelen voldoende omdat het risico voor betrokkene bij verlies, onbevoegd of onzorgvuldig gebruik beperkt is. Het gaat hierbij meestal om beperkte aantallen gegevens die over het algemeen alleen maar betrekking hebben op de relatie tussen een organisatie en de betrokkene (zoals lidmaatschappen, arbeidsovereenkomsten, huurcontracten etc.). Aandachtspunt hierbij moet wel zijn dat de gegevens uit deze klasse informatie in zich kunnen dragen die informatie geeft over een persoon waarbij de informatie als zodanig valt onder de categorie bijzondere gegevens (zoals het lidmaatschap van een kerkelijk genootschap of bepaalde dieetgegevens die aanduidingen bevatten over het geloof van de betrokkene). Is dit het geval dan horen deze verwerkingen niet thuis in deze risicoklasse maar minimaal in klasse II
Criterium om in klasse I te vallen is dus: beperkt aantal gegevens van een standaard inhoud.

Risicoklasse II: verhoogd risico
Verlies, onzorgvuldig gebruik of onbehoorlijke verwerking van gegevens uit deze categorie heeft extra negatieve gevolgen voor betrokkene. De meest heldere afbakening hiervoor ligt in de artikelen 16 tot en met 23; zo gauw er sprake is van verwerking van bijzondere gegevens is er sprake van een verhoogd risico. Ook gegevens die betrekking hebben op de persoonlijke, financiële of economische situatie van betrokkene verdienen de bescherming van deze risicoklasse. Het hoeft echter niet alleen zo te zijn dat één betrokkene de extra negatieve gevolgen ondervindt. Ook indien grote groepen de

[108] G. van Blarkom, J. Leerentveld en R. Schreijnders (red.), Raamwerk privacy audit, Den Haag, CBP, april 2001, pag. 39; G.W van Blarkom, J.J. Borking, Beveiliging van persoonsgegevens, Den Haag, Registratiekamer, april 2001, pag. 20.
[109] Kamerstukken Eerste Kamer, vergaderjaar 1999-2000, 25 892, nr. 31.
[110] G.W van Blarkom, J.J. Borking, Beveiliging van persoonsgegevens, Den Haag, Registratiekamer, april 2001, pag. 26 e.v.

impact kunnen voelen van verwerkingen van relatief onschuldige gegevens is er sprake van verhoogd risico.
Criterium om in risicoklasse II te vallen is dus de verwerking van bijzondere gegevens of de verwerking van grote hoeveelheden standaardgegevens.

Risicoklasse III: hoog risico
Verwerking van dit type gegevens heeft het risico in zich dat de belangen van betrokkenen ernstig kunnen worden geschaad. Ook gegevens waarop bijzondere geheimhoudingsverplichtingen van toepassing zijn vallen in deze klasse. Zelfs gegevens die normaliter in klasse III zouden vallen maar door hun hoge gevoeligheidsgraad in het maatschappelijke verkeer de belangen van betrokkene ernstig zouden kunnen schaden dienen in deze klasse te worden opgenomen.
Criterium om in deze hoogste klasse te worden opgenomen is dus de bijzonderheid van de gegevens, een grote hoeveelheid gegevens of een additionele plicht tot geheimhouding.

Nu er een structuur is waarin de diverse geïnventariseerde verwerkingen kunnen worden ondergebracht dient nog per risicoklasse het passende beveiligingsniveau[111] te worden vastgesteld. Het begrip beveiliging wordt hiervoor opgedeeld in een 14-tal deelgebieden[112] waarbinnen concrete maatregelen en/of niveaus per risicoklasse kunnen worden vastgesteld. Een aantal van de te behalen niveaus zijn inmiddels al tot norm verheven[113]. Binnen dit onderzoek zullen de uitgangspunten zoals die in deze NEN-norm zijn opgenomen dan ook primair als toetsingscriteria voor beveiliging worden gebruikt[114].

6.6.2 Beveiligingsbeleid

Informatiebeveiliging is pas effectief als dit op een gestructureerde manier wordt aangepakt. De basis hiervoor moet liggen in het beleid zoals dat door de leiding van een organisatie tot uiting wordt gebracht. De hoofdelementen van dit beleid moeten aandacht geven aan de te bereiken doelen, de manier waarop deze doelen moeten worden bereikt, de verantwoordelijkheden van de medewerkers hierin en de wijze waarop wordt gecontroleerd of de gestelde doelen zijn bereikt[115]. De criteria waarop de inhoud van dit beleidsdocument moet worden beoordeeld zijn onderdeel van de NEN-7510[116] en luiden als volgt:

Criteria
1. Is binnen uw organisatie[117] afgesproken (en vastgelegd) hoe met informatiebeveiliging wordt omgegaan (wat wordt eraan gedaan en wat willen we eraan doen)?
2. Is afgesproken wie er eindverantwoordelijk is voor het onderwerp binnen uw organisatie?
3. Wordt regelmatig bekeken wat er van de plannen op het gebied van informatiebeveiliging binnen uw organisatie is terechtgekomen?
4. Is er een beleidsdocument voor informatiebeveiliging opgesteld met als aandachtsgebied de organisatie en de aangeslotenen?
5. Vindt periodiek een beoordeling en evaluatie plaats van het totale informatiebeveiligingsbeleid?

[111] "Een passend beveiligingsniveau is een vereiste om gegevens uit te wisselen. Als uitgangspunt daarvoor zal de recent vastgestelde norm voor informatiebeveiliging in de zorg gaan gelden, de NEN 7510"; Tweede Kamer, vergaderjaar 2004–2005, 29 800 hoofdstuk XVI, nr. 2, pag. 134.
[112] Conform de indeling uit AV23; G.W van Blarkom, J.J. Borking, Beveiliging van persoonsgegevens, Den Haag, Registratiekamer, april 2001, pag. 32 e.v.
[113] NEN 7510, Delft, Nederlands Normalisatie Instituut, april 2004.
[114] Deze keuze heeft, naast de praktische structuur die voor dit onderzoek wordt geboden, nog een toekomstgericht voordeel; de IGZ heeft aangekondigd in 2005 de ziekenhuizen en verpleeghuizen te controleren op naleving van het gestelde in de NEN-7510. Het gebruik van de criteria uit de norm in dit onderzoek leidt dus ook tot een overzicht dat gebruikt kan worden tijdens de controle van de IGZ.
[115] G.W van Blarkom, J.J. Borking, Beveiliging van persoonsgegevens, Den Haag, Registratiekamer, april 2001, pag. 32.
[116] NEN 7510, Delft, Nederlands Normalisatie Instituut, april 2004, pag. 12-13 en G.W van Blarkom, J.J. Borking, Beveiliging van persoonsgegevens, Den Haag, Registratiekamer, april 2001, pag. 32-34.
[117] De implementatiehulpmiddelen van de NEN-7510 gebruiken hier het begrip "netwerkorganisatie". Binnen dit onderzoek is deze term niet overgenomen maar verdeeld in drie andere: organisatie in de zin van De Vitalis Zorg Groep, aangeslotenen in de zin van alle gebruikers van het computernetwerk en ICT-organisatie in de zin van de ICT-afdeling, verantwoordelijk voor beleid, implementatie en beheer van de ICT-middelen.

6.6.3 Organiseren van informatiebeveiliging

Informatiebeveiliging is in de basis mensenwerk en is dus alleen mogelijk indien alle partijen die invloed kunnen uitoefenen op het niveau van de beveiliging zich bewust zijn van hun taken en bevoegdheden en het voor eenieder duidelijk is wie waarvoor verantwoordelijk is. Dit is niet alleen van toepassing op de eigen organisatie maar op iedereen die toegang heeft tot de systemen van de organisatie of gegevens verwerkt. Om dit te bereiken is het niet alleen van belang dat maatregelen en processen op een gestructureerde manier worden beschreven maar ook dat steeds gecontroleerd dient te worden of de beschreven procedures en maatregelen nog goed aansluiten bij de dagelijkse praktijk en eventueel gewijzigde omstandigheden[118]. De volgende criteria worden hiervoor gegeven:

Criteria

1. Is binnen de organisatie besproken wie verantwoordelijk is voor het in gebruik nemen van nieuwe IT-middelen (of andere informatiemiddelen).
2. Zijn er met 'derden' (zoals onderhoudspersonen hard- en software, schoonmaakpersoneel, tijdelijke krachten) afspraken gemaakt over toegang tot ruimten en informatiemiddelen?
3. Als ICT-activiteiten zijn uitbesteedt, is er dan in contracten duidelijkheid over informatiebeveiliging?
4. Wordt er aandacht besteedt aan opleiding van medewerkers voor wat betreft informatiebeveiliging?
5. Beschikt de organisatie over een beveiligingsadviseur of een contactpersoon voor informatiebeveiliging?
6. Heeft de beveiligingsadviseur of de contactpersoon voor informatiebeveiliging contacten met andere beveiligingsadviseurs uit bedrijfsleven of overheid?
7. Is een multidisciplinair forum aanwezig, bestaande uit managers of afgevaardigden van alle aangeslotenen en de ICT-organisatie zelf, die de implementatie van maatregelen voor informatiebeveiliging coördineert?
8. Zijn de verantwoordelijkheden voor de bescherming van individuele bedrijfsmiddelen en voor het uitvoeren van bepaalde beveiligingsprocessen duidelijk gedefinieerd?
9. Wordt de implementatie van de informatiebeveiliging regelmatig beoordeeld door een onafhankelijke instantie?
10. Worden de risico's geanalyseerd die ontstaan doordat externe gebruikers (aangeslotenen) fysieke en/of logische toegang hebben tot informatieverwerkende voorzieningen?
11. Zijn beveiligingseisen gespecificeerd in contracten met derden die betrekking hebben op de toegang tot de informatieverwerkende voorzieningen van de organisatie?
12. Worden beveiligingseisen opgenomen in de uitbestedingscontracten met derden?

6.6.4 Beheer van middelen voor informatievoorziening

Voor de bedrijfsvoering is het belangrijk dat een verwerkende organisatie overzicht heeft over de actuele status van alle middelen, mensen, gegevensverzamelingen[119], procedures en documentatie die voor de informatievoorziening worden gebruikt. De concrete eisen die aan de diverse onderdelen van de informatievoorziening worden gesteld, hangen af van de risico's die aan de verwerking van de specifieke gegevens kleven (zie pag. 28 e.v. voor de methodiek van het vaststellen van de risicoklasse).
De eerste eis is die van overzicht van alle betrokkene middelen. Dit overzicht moet bevatten welke middelen gebruikt worden, waar deze zich bevinden, wie de verantwoordelijkheid hierover heeft en wie is geautoriseerd voor gebruik. Omdat de noodzakelijke beveiligingsniveaus afhangen van de verschillende soorten gegevens, ontstaat de noodzaak tot classificatie van gegevens zoals in de inleiding van deze paragraaf al aangegeven. Deze classificatie dient regelmatig geëvalueerd te worden[120]. De volgende criteria zijn uit deze beveiligingseisen af te leiden:

[118] G.W van Blarkom, J.J. Borking, Beveiliging van persoonsgegevens, Den Haag, Registratiekamer, april 2001, pag. 33 en NEN 7510, Delft, Nederlands Normalisatie Instituut, april 2004, pag. 13-14.
[119] De inventarisatie van bestaande verzamelingen is het eerste deel van dit onderzoek en wordt hier niet verder uitgewerkt. Door een eenduidige inventarisatie uit te voeren is aan dit onderdeel van de beveiligingseisen voldaan.
[120] G.W van Blarkom, J.J. Borking, Beveiliging van persoonsgegevens, Den Haag, Registratiekamer, april 2001, pag. 41 en NEN 7510, Delft, Nederlands Normalisatie Instituut, april 2004, pag. 16-17.

Criteria
1. Is voor alle informatievoorzieningmiddelen (computers, faxen, netwerkinfrastructuur, etc.) afgesproken wie er verantwoordelijk is voor onderhoud, integriteit enzovoorts?
2. Wordt bij het beveiligen van informatie onderscheid gemaakt voor wat betreft het soort informatie waar het over gaat (b.v. heel vertrouwelijk versus voor iedereen toegankelijk)?
3. Maakt men gebruik van beveiligingsclassificaties voor kritische en gevoelige informatie, teneinde het vereiste beveiligingsniveau te kunnen aangeven?
4. Zijn er over het omgaan met die soorten informatie afspraken vastgelegd?

6.6.5 Beveiligingseisen ten aanzien van personeel

Deze eisen zijn er op gericht de risico's van menselijke fouten bij de verwerking van persoonsgegevens te verminderen. De mogelijkheid is altijd aanwezig dat een (nieuwe) medewerker, bewust of onbewust, onzorgvuldig is bij de omgang met persoonsgegevens. Om deze risico's te beperken is het belangrijk dat er gedurende de gehele loopbaan van de medewerker maar met name al bij het begin (werving, selectie en aanname) aandacht wordt besteed aan opleiding en training, gericht op beveiliging van persoonsgegevens.
In de sollicitatiefase kan het noodzakelijk zijn extra inlichtingen in te winnen over de medewerkers, waarbij de detaillering van de gewenste inlichtingen (referenties, antecedentenonderzoek of zelfs een verklaring van goed gedrag) gerelateerd moet zijn aan de risicoklasse van de persoonsgegevens waarmee de medewerker in aanraking zal komen. Ook binnen de uitoefening van de functie zal aandacht besteedt moeten worden aan beveiliging. Zo zal het onmogelijk moeten zijn dat een medewerker onverenigbare taken vervult voor wat betreft beveiliging (functiescheiding). Daarnaast zal een medewerker in een aantal gevallen een additionele geheimhoudingsverklaring moeten tekenen om toegang te krijgen tot persoonsgegevens. Uiteraard moeten alle na te leven richtlijnen met betrekking tot gebruik en beveiliging van persoonsgegevens duidelijk zijn voor alle medewerkers zodat zij weten wat er van hun wordt verwacht, eventueel gecombineerd met additionele trainingen en nascholing. Mocht een medewerker bewust de beveiliging doorbreken, dan moet er een corrigerend of disciplinair proces beschikbaar zijn voor de organisatie.
Na vertrek van een medewerker moet er duidelijkheid zijn over de mogelijkheden die beschikbaar blijven om alsnog toegang te krijgen tot de informatie(systemen) van de organisatie en welke beveiligingen hiertegen kunnen worden ingezet. De volgende criteria voor beveiligingseisen ten aanzien van personeel zijn hieruit af te leiden[121]:

Criteria
1. Zijn beveiligingstaken en -verantwoordelijkheden, zoals vastgelegd in het beveiligingsbeleid, opgenomen in functieomschrijvingen?
2. Worden sollicitanten naar een functie waarbij men toegang heeft tot gevoelige informatie, gescreend alvorens zij worden aangenomen?
3. Moeten medewerkers een geheimhoudingsverklaring ondertekenen?
4. Is in het arbeidscontract opgenomen dat de medewerker een verantwoordelijkheid heeft op het gebied van informatiebeveiliging?
5. Wordt er binnen de organisatie aandacht besteedt in het overbrengen van het hoe en wat met betrekking tot informatiebeveiliging op de medewerkers?
6. Worden alle aangeslotenen op passende wijze getraind in beveiligingsprocedures en de bijbehorende technieken?
7. Zijn binnen de organisatie afspraken gemaakt over hoe om te gaan met beveiligingsincidenten?
8. Worden beveiligingsincidenten op de een of andere manier vastgelegd?
9. Zijn procedures vastgesteld voor het melden door de aangeslotenen en afhandelen van beveiligingsincidenten?
10. Zijn de aangeslotenen verplicht om alle zwakke plekken, die zij opmerken of vermoeden in de beveiliging van systemen of diensten van de ICT-organisatie, te noteren en te rapporteren?
11. Is een mechanisme aanwezig dat de organisatie in staat stelt de aard, de omvang en de kosten van incidenten en storingen te kwantificeren en te bewaken?
12. Worden inbreuken op de beveiliging door middel van een formeel disciplinair proces afgehandeld?

[121] G.W van Blarkom, J.J. Borking, Beveiliging van persoonsgegevens, Den Haag, Registratiekamer, april 2001, pag. 38 en NEN 7510, Delft, Nederlands Normalisatie Instituut, april 2004, pag. 17-19.

6.6.6 Fysieke beveiliging en beveiliging van de omgeving

Het is noodzakelijk dat een instelling de ruimten en apparatuur die betrokken zijn bij de informatievoorziening beveiligt. Juist in zorginstellingen, waarbij immers veel van de ruimten vrij toegankelijk zijn, is fysieke toegangsbeveiliging en logische systeembeveiliging van belang. Het beveiligen van een compleet terrein van een instelling is niet mogelijk, juist gezien dit publieke karakter, en dus moeten zones en ruimtes worden gedefinieerd binnen een instelling waartoe slechts geautoriseerd personeel toegang heeft en welke toegang ook eenduidig vastgelegd en gecontroleerd wordt. Naast toegangscontrole is ook beveiliging tegen schade, brand en andere calamiteiten van belang. Informatiesystemen moeten worden beschermd tegen invloeden van buitenaf, waarbij deze bescherming niet alleen moet gelden voor de systemen zelf maar ook voor stroomvoorzieningen, communicatiebekabeling en systemen die in opslag staan of afgevoerd worden. Maatregelen en procedures voor fysieke beveiliging moeten eenduidig zijn vastgelegd en uiteraard ook gelden voor derden die werkzaam zijn binnen de organisatie.
De volgende criteria met betrekking tot beveiliging zijn hieruit af te leiden[122]:

Criteria

1. Maakt de organisatie onderscheid naar verschillende beveiligingsniveaus om gebieden die IT-voorzieningen bevatten te beschermen?
2. Worden beveiligde zones beschermd door een adequate toegangsbeveiliging, zodat alleen geautoriseerd personeel toegang heeft?
3. Wordt bij de keuze en het ontwerp van een beveiligde zone rekening gehouden met de mogelijkheid van schade door fysieke bedreigingen, zoals brand, wateroverlast, explosie en dergelijke?
4. Zijn additionele richtlijnen en maatregelen aanwezig om de beveiliging van beveiligde ruimten te kunnen waarborgen?
5. Wordt apparatuur zodanig geplaatst en beveiligd dat de risico's van schade, storing en ongeautoriseerd gebruik minimaal zijn?
6. Is apparatuur beveiligd tegen stroomstoringen en andere elektrische storingen?
7. Is de bekabeling voor dataverkeer en voor ondersteunende informatiediensten beschermd tegen interceptie of beschadiging?
8. Wordt alle apparatuur op correcte wijze onderhouden?
9. Gelden beveiligingsprocedures en beveiligingsmaatregelen ook voor apparatuur die, door de medewerker buiten de organisatie wordt gebruikt?
10. Wordt apparatuur gecontroleerd op de aanwezigheid van opgeslagen gegevens en in licentie gebruikte software, voordat de apparatuur wordt afgevoerd?
11. Is een *clear desk* en *clear screen policy* ingevoerd?
12. Zijn maatregelen getroffen om te voorkomen dat het personeel zonder toestemming eigendommen van de organisatie meeneemt?

6.6.7 Operationeel beheer van voorzieningen

Om een correcte en veilige bediening van ICT-systemen[123] te kunnen waarborgen en de beschikbaarheid en integriteit van apparatuur, gegevens en (communicatie)diensten te beschermen, is eenduidige vastlegging van procedures en verantwoordelijkheden een eerste vereiste.
Een onderdeel hiervan is de beschrijving van de bedieningsprocedures en de bij uitvoering horende verantwoordelijkheden van personeel. Alle procedures dienen te zijn beschreven en wijzigingen, zowel op procedures als op systemen, moeten worden vastgelegd in logboeken. Binnen de personele bevoegdheden moeten bepaalde taken worden verdeeld over meerdere personen zodat misbruik van systeembevoegdheden wordt uitgesloten.

Indien taken zijn uitbesteed aan derden moeten de passende maatregelen contractueel zijn vastgelegd en regelmatig worden gecontroleerd op naleving door de verantwoordelijke. Zoals reeds kort aangestipt in de inleiding in paragraaf 6.6.1 legt de derde beveiligingseis uit artikel 13 WBP de

[122] G.W van Blarkom, J.J. Borking, Beveiliging van persoonsgegevens, Den Haag, Registratiekamer, april 2001, pag. 43 en NEN 7510, Delft, Nederlands Normalisatie Instituut, april 2004, pag. 19-21.
[123] Het begrip “ICT-systemen” wordt hier gebruikt in de breedste zin van het woord: alle computersystemen en -netwerken, systeem- en toepassingssoftware, de gegevens op de systemen, mensen, documentatie en procedures welke van toepassing zijn op de verwerking van persoonsgegevens. Zie G.W van Blarkom, J.J. Borking, Beveiliging van persoonsgegevens, Den Haag, Registratiekamer, april 2001, pag. 41.

verantwoordelijkheid voor verwerkingen die zijn uitbesteed aan een derde neer bij de eerstverantwoordelijke van de oorspronkelijke verwerking: de opdrachtgever. Deze verantwoordelijke heeft de zorgplicht de bewerker duidelijk te maken hoe met de ter bewerking aangeboden persoonsgegevens dient te worden omgegaan, maar dient ook toe te zien op de feitelijke naleving van de aangegane verplichtingen[124]. Op basis hiervan kan al een aantal eisen worden geformuleerd waaraan een bewerker en de relatie met deze bewerker moet voldoen[125]. De eerste is de controle die de verantwoordelijke moet uitvoeren of de bewerker voldoet aan de eisen van artikel 13 WBP ofwel afdoende technische en organisatorische maatregelen voor beveiliging heeft getroffen zoals deze in de voorgaande en volgende paragrafen zijn uitgewerkt. Daarnaast moet de relatie met de bewerker zijn vastgelegd in een overeenkomst waaruit rechtens afdwingbare verbintenissen ontstaan. Deze overeenkomst moet onder andere de opdracht aan de bewerker bevatten dat deze de persoonsgegevens slechts in opdracht van de verantwoordelijke mag verwerken en dat de verantwoordelijke het recht heeft de verwerkingen te toetsen op naleving van de beveiligingsverplichtingen[126].

Om de werking van de operationele systemen veilig te stellen zullen test- en ontwikkelsystemen gescheiden moeten worden opgesteld en dient de acceptatie van nieuwe systemen evenals de overdracht van de ene naar de andere omgeving te worden getoetst. Uiteraard moeten er op de operationele systemen maatregelen zijn getroffen om deze te beschermen tegen verlies van gegevens (back-up) en invloeden van kwaadaardige of destructieve programmatuur (virus). Van alle getroffen beheers- en beveiligingsmaatregelen moeten duidelijke overzichten en beschrijvingen beschikbaar zijn.
Opgeslagen gegevens moeten worden beschermd tijdens noodzakelijke transporten, zowel over het netwerk als bij gebruik van losse media waarbij het “opschonen” van losse gegevensdragers extra aandacht behoeft[127]. Bij opslag en transport over netwerken moeten er maatregelen getroffen zijn om de gegevens te beschermen tegen de risico’s van onvolledige overdracht, ongeautoriseerde toegang, ongeoorloofde wijzigingen en verkeerd terechtkomen[128].
Uit dit overzicht van voorwaarden voor beheer zijn de volgende criteria af te leiden:

Criteria
1. Zijn schriftelijke procedures opgesteld voor de bediening van alle IT-voorzieningen?
2. Zijn formele procedures aanwezig met betrekking tot de controle op wijzigingen in IT-voorzieningen en informatiesystemen?
3. Is bepaald wie wat mag met betrekking tot het toevoegen, wijzigen en verwijderen van informatie?
4. Zijn verantwoordelijkheden en procedures vastgesteld voor de afhandeling van beveiligingsincidenten?
5. Wordt functiescheiding toegepast om de kans op ongeautoriseerde wijzigingen of opzettelijk misbruik van informatie of diensten te verkleinen?
6. Zijn de voorzieningen voor het ontwikkelen en testen van systemen gescheiden van operationele systemen?
7. Zijn, in het geval van uitbesteding van het beheer van IT-voorzieningen, passende beveiligingsmaatregelen met de contractant overeengekomen en zijn deze opgenomen in het contract?
8. Worden de capaciteitseisen *gemonitored* en wordt een prognose gemaakt van toekomstige eisen, teneinde storingen ten gevolge van een gebrek aan capaciteit te voorkomen?
9. Worden acceptatiecriteria gedefinieerd, besproken, gedocumenteerd en getest alvorens nieuwe informatiesystemen te accepteren?
10. Zijn maatregelen ingevoerd voor de preventie en detectie van kwaadaardige software, zoals virussen?
11. Worden regelmatig reservekopieën gemaakt van essentiële zakelijke informatie en software?
12. Houden de systeembeheerders een logboek bij van de werkzaamheden die zij verrichten?
13. Worden de, door de aangeslotenen gemelde, storingen vastgelegd in een logboek?

[124] J. Nouwt, Invoering van de WBP in tien stappen, http://rechten.uvt.nl/sjaaknouwt/Zorgvisi.doc , pag. 3.
[125] G. van Blarkom, J. Leerentveld en R. Schreijnders (red.), Raamwerk privacy audit, Den Haag, CBP, april 2001, pag. 40.
[126] L.B. Sauerwein en J.J. Linneman, Handleiding voor verwerkers van persoonsgegevens, Den Haag, Ministerie van Justitie, 2001, pag. 43.
[127] Opschonen van afgeschreven gegevensdragers is een “hot-item” gezien de recente nieuwsberichten over computers die niet opgeschoond aan de straat zijn gezet.
[128] G.W van Blarkom, J.J. Borking, Beveiliging van persoonsgegevens, Den Haag, Registratiekamer, april 2001, pag. 41 en NEN 7510, Delft, Nederlands Normalisatie Instituut, april 2004, pag. 21-25.

14. Zijn adequate maatregelen getroffen voor de beveiliging van gegevens in netwerken en de bescherming van de aangeslotenen tegen ongeautoriseerde toegang?
15. Zijn procedures opgesteld voor het beheer van verwijderbare computermedia zoals banden, schijven, cassettes en afgedrukte rapporten?
16. Worden media op een veilige manier afgevoerd wanneer zij niet langer nodig zijn?
17. Zijn procedures opgesteld voor de behandeling en opslag van informatie ter bescherming tegen ongeoorloofde openbaarmaking of misbruik?
18. Is systeemdocumentatie beveiligd tegen ongeautoriseerde toegang?
19. Zijn in overeenkomsten met de aangeslotenen en 'derden' beveiligingsmaatregelen met betrekking tot het uitwisselen van informatie en software opgenomen?
20. Zijn maatregelen genomen ter beveiliging van computermedia tijdens vervoer tegen misbruik of verlies?
21. Zijn speciale maatregelen getroffen ter beveiliging van elektronische handel die nodig kunnen zijn om o.a. frauduleuze handelingen, contractgeschillen en ongewilde openbaring of manipulatie van informatie te voorkomen?
22. Zijn speciale maatregelen getroffen voor de beperking van de risico's van het gebruik van elektronische post?
23. Zijn duidelijke richtlijnen en procedures opgesteld voor de beheersing van de risico's die elektronische kantoorsystemen met zich meebrengen?
24. Is aandacht besteed aan de bescherming van de integriteit van elektronisch gepubliceerde informatie, om te voorkomen dat de reputatie van de uitgevende organisatie beschadigd raakt doordat ongeautoriseerde wijzigingen plaatsvinden?

6.6.8 Toegangsbeveiliging

Naast fysieke beveiliging van de omgeving en de systemen zoals beschreven in paragraaf 6.6.6 is ook logische beveiliging van informatiesystemen een belangrijk onderdeel van de beveiligingseisen. Hieronder valt een duidelijke regeling voor het gebruik van wachtwoorden, het toekennen, veranderen of intrekken van autorisaties en het vastleggen wie op welk moment toegang heeft gehad tot persoonsgegevens *(audit-trail).* Uitgangspunt moet zijn dat de toegang tot gegevens zoveel mogelijk moet worden beperkt, echter deze eis kan conflicteren met de gewenste beschikbaarheid van gegevens. Met name in acute situaties zoals deze in de zorg kunnen voorkomen is het van belang dat toegang tot gegevens mogelijk is, waardoor het in sommige gevallen noodzakelijk kan zijn reguliere toegangsbeveiligingen te doorbreken. Deze optie vraagt enerzijds duidelijke criteria voor wanneer er sprake is van een situatie die het doorbreken van beveiligingen rechtvaardigt maar eist aan de andere kant de mogelijkheid om achteraf de acties te reconstrueren en te controleren.
Een eerste stap in het bereiken hiervan is een eenduidige registratie en identificatie van gebruikers alsmede registratie van de apparatuur waarmee deze gebruikers toegang tot de systemen mogen krijgen. Identificatie van gebruikers moet minimaal bestaan uit de combinatie van een unieke ID in combinatie met een wachtwoord. Naarmate de risicoklasse van de gegevens hoger is zullen aanvullende methoden van identificatie en authenticatie moeten worden toegepast.
Gebruikers moeten zich bewust zijn van de risico's van onverantwoord omgaan met wachtwoorden en moeten verantwoordelijk gesteld kunnen worden voor misbruik van hun toegangscodes. Voor communicatie tussen systemen gelden in principe dezelfde eisen hetgeen wil zeggen dat apparaten zich op basis van unieke codes aan elkaar bekend moeten stellen.
Apparatuur die onderdeel is van ICT-systemen dient in principe nooit onbeheerd te zijn maar aangezien deze eis op praktische problemen kan stuiten dienen er procedures dan wel instellingen te zijn die het gebruik van onbeheerde systemen onmogelijk maken *(time-out).* Alle bovengenoemde maatregelen moeten eenduidig in procedures zijn beschreven.
Uit deze opsomming van eisen[129] aan de logische toegangsbeveiliging van systemen zijn de volgende criteria af te leiden:

Criteria

1. Wordt er gebruik gemaakt van 'autorisatieprofielen' (welke medewerker mag wat) met betrekking tot toegang tot informatie en IT-middelen?
2. Is er een noodprocedure die toegang in noodgevallen regelt?

[129] G.W van Blarkom, J.J. Borking, Beveiliging van persoonsgegevens, Den Haag, Registratiekamer, april 2001, pag. 43 en NEN 7510, Delft, Nederlands Normalisatie Instituut, april 2004, pag. 25-28.

3. Is een beleid vastgesteld ten aanzien van toegangsbeveiliging waarin de eisen en de regels voor toegangsbeveiliging zijn vastgelegd?
4. Zijn formele procedures opgesteld voor het registreren en afmelden van aangeslotenen voor toegang tot informatiesystemen en -diensten met meerdere gebruikers?
5. Worden speciale bevoegdheden aan de hand van formele autorisatieprocedures verleend?
6. Is er een formeel proces ingericht voor de toewijzing van wachtwoorden aan medewerkers van de ICT-organisatie?
7. Is er een formeel proces ingericht voor de toewijzing van wachtwoorden aan de aangeslotenen?
8. Worden de uitgegeven toegangsrechten van de medewerkers van de ICT-organisatie regelmatig gecontroleerd?
9. Worden de uitgegeven toegangsrechten van de aangeslotenen regelmatig gecontroleerd?
10. Worden de aangeslotenen verplicht om de beveiligingsregels ten aanzien van het kiezen en gebruiken van wachtwoorden in acht te nemen?
11. Zorgen de medewerkers ervoor dat onbeheerde apparatuur voldoende is beveiligd?
12. Is een beleid geformuleerd ten aanzien van het gebruik van netwerken en netwerkdiensten?
13. Wordt de route van het werkstation naar de servers beheerst?
14. Kan op afstand op de systemen van de ICT-organisatie worden ingelogd (door medewerkers of 'derden' zoals leveranciers)?
15. Is de toegang van de aangeslotenen op afstand via externe verbindingen beveiligd door middel van een authenticatieprocedure?
16. Verloopt de toegang door de medewerkers van de ICT-organisatie tot informatiediensten via een veilig aanlogproces?
17. Worden verbindingen die door computersystemen op afstand tot stand worden gebracht, geauthenticeerd?
18. Zijn beveiligingsmaatregelen getroffen voor de beheersing van de toegang tot diagnosepoorten?
19. Zijn grote netwerken opgesplitst in afzonderlijke domeinen?
20. Zijn maatregelen getroffen voor de beperking van de verbindingsmogelijkheden voor de aangeslotenen teneinde de toegangsvereisten voor bepaalde bedrijfstoepassingen te ondersteunen?
21. Zijn in gemeenschappelijke netwerken beveiligingsmaatregelen voor netwerkrouting getroffen?
22. Heeft de netwerkleverancier een duidelijke beschrijving gegeven van alle beveiligingskenmerken van de gebruikte netwerkservices?
23. Wordt een automatisch identificatiesysteem voor werkstations gebruikt om de verbindingen met specifieke locaties en mobiele apparatuur te verifiëren?
24. Verloopt de toegang door de aangeslotenen tot informatiediensten via een veilig aanlogproces?
25. Zijn alle computeractiviteiten tot een individuele aangeslotene terug te voeren?
26. Wordt gebruik gemaakt van een effectief en interactief wachtwoordmanagementsysteem?
27. Zijn maatregelen getroffen voor de beheersing van het gebruik van systeemhulpmiddelen?
28. Is voor alle medewerkers van de organisatie, die de kans lopen het doelwit van dwang of bedreiging te worden, een stil alarm ingevoerd?
29. Is voor inactieve werkstations op locaties met verhoogd risico een time-out voorziening ingesteld?
30. Is de verbindingstijd door de aangeslotenen voor toepassingen met een verhoogd risico beperkt?
31. Worden bepaalde gevoelige toepassingssystemen in een vast toegewezen (geïsoleerde) computeromgeving uitgevoerd?
32. Wordt ergens bijgehouden (in een log-bestand van de software) wie wat gedaan heeft op het informatiesysteem?
33. Zijn procedures voor de *monitoring* van systeemgebruik vastgesteld?
34. Worden systeemklokken gesynchroniseerd teneinde (log)gegevens nauwkeurig te kunnen vastleggen?
35. Is een formeel beleid opgesteld voor de omgang met mobiele systemen welke de risico's behandelt van het werken met mobiele computervoorzieningen?
36. Beschikt de organisatie over een beleid, procedures en normen voor de beheersing van activiteiten op het gebied van telewerken?

6.6.9 Aanschaf, ontwikkeling en onderhoud van systemen

Dit onderdeel van informatiebeveiliging is onder te verdelen in twee aandachtsgebieden. Ten eerste moet bij aanschaf, ontwikkeling en beheer er voor gezorgd worden dat de nieuwe systemen zelf voldoen aan de noodzakelijke functionele beveiligingseisen. Systemen zijn niet in alle gevallen foutvrij

waardoor de mogelijkheid bestaat dat opgeslagen persoonsgegevens verloren gaan, onjuist zijn of onbedoeld worden veranderd. Ook kunnen fouten in software er toe leiden dat bestaande beveiligingen kunnen worden omzeild. Het verdient de voorkeur dat de beveiliging voor systemen een integraal onderdeel uitmaakt van het informatiesysteem waarbij vooraf, op basis van een risicoanalyse (zie paragraaf 6.6), het gewenste niveau van beveiliging is vastgesteld. Uiteraard zal de beveiliging moeten voldoen aan de (minimale) wettelijke eisen maar zal ook moeten aansluiten bij de wensen van de organisatie (zie onder andere de het dilemma tussen adequate beveiliging en de noodzaak tot toegang in noodgevallen in de vorige paragraaf).
Voor toepassingssoftware moeten mechanismen beschikbaar zijn die invoer, verwerking en uitvoer controleren op juistheid, volledigheid en mate van actualiteit. Als gegevens elektronisch worden getransporteerd moeten er maatregelen getroffen zijn die er voor zorgen dat afzender en ontvanger eenduidig zijn geïdentificeerd en geauthenticeerd. Naast authenticatie zullen er ook maatregelen genomen moeten zijn die gericht zijn op het voorkomen van openbaarmaking van berichten die “op transport” zijn waarbij elektronische handtekeningen, sterke authenticatie en versleuteling (encryptie) tot de mogelijkheden behoren.

Ten tweede moet ook het proces van aanschaf, ontwikkeling en onderhoud zelf voldoende zijn beveiligd. Wijzigingen in de software moeten worden gedocumenteerd en goedgekeurd en toegang tot oorspronkelijke software moet gewaarborgd zijn. Bij systemen die ingezet worden bij de verwerking van gevoelige gegevens kan het zelfs noodzakelijk zijn deze vooraf door onafhankelijke partijen te laten evalueren en testen om er zeker van te zijn dat deze voldoen aan de gestelde eisen van informatiebeveiliging. Bij wijzigingen in systeemprogrammatuur zullen zelfs alle systemen die hiervan gebruik maken opnieuw beoordeeld dienen te worden op relevante beveiligingaspecten van verwerking en toegang. Uit dit overzicht[130] van aandachtspunten voor aanschaf, ontwikkeling en onderhoud kunnen de volgende criteria worden afgeleid:

Criteria:
1. Wordt een analyse van de beveiligingseisen uitgevoerd tijdens het specificeren van de eisen voor een te ontwikkelen informatiesysteem?
2. Worden gegevens die worden ingevoerd in toepassingssystemen gevalideerd op juistheid en geschiktheid?
3. Zijn maatregelen getroffen voor de validatie van de interne gegevensverwerking?
4. Wordt authenticatie van berichten toegepast voor toepassingen waarbij de bescherming van de inhoud van berichten essentieel is?
5. Worden controles uitgevoerd op de uitvoergegevens om te verifiëren of de verwerking van de opgeslagen gegevens juist is verlopen?
6. Is een beleid aanwezig voor het gebruik van cryptografische technieken voor de beveiliging van gegevens?
7. Wordt versleuteling toegepast voor de bescherming van gevoelige informatie?
8. Wordt voor de waarborging van de authenticiteit en de integriteit van elektronische documenten gebruik gemaakt van digitale handtekeningen?
9. Wordt gebruik gemaakt van diensten die de onweerlegbaarheid kunnen aantonen van gebeurtenissen, om eventuele meningsverschillen uit de weg te ruimen over het bestaan van deze gebeurtenissen?
10. Is een managementsysteem aanwezig voor het beheer van cryptografische sleutels?
11. Wordt de implementatie van software op operationele systemen nauwkeurig beheerst?
12. Zijn maatregelen getroffen voor de beveiliging en het beheer van testgegevens?
13. Zijn maatregelen getroffen voor de toegangsbeveiliging van softwarebibliotheken?
14. Zijn formele procedures opgesteld voor het beheer van wijzigingen in informatiesystemen?
15. Worden de gevolgen voor de beveiliging van alle wijzigingen in het besturingssysteem nagegaan?
16. Worden wijzigingen in softwarepakketten zoveel mogelijk vermeden?
17. Zijn maatregelen getroffen ter voorkoming van de opname van Trojaanse paarden en geheime communicatiekanalen in informatiesystemen?
18. Is een beleid geformuleerd voor het uitbesteden van de ontwikkeling van programmatuur?

[130] G.W van Blarkom, J.J. Borking, Beveiliging van persoonsgegevens, Den Haag, Registratiekamer, april 2001, pag. 47 en NEN 7510, Delft, Nederlands Normalisatie Instituut, april 2004, pag. 28-32.

6.6.10 Continuïteitsbeheer

Elke verwerkende organisatie kan geconfronteerd worden met onvoorziene omstandigheden en calamiteiten die de bedrijfsvoering kunnen onderbreken. In extreme gevallen kan hierdoor zelfs de continuïteit van de organisatie in gevaar worden gebracht. Voor verwerkingen van persoonsgegevens kan dit betekenen dat deze beschadigd zijn of ontoegankelijk zijn geworden. Om de verstoringen als gevolg van calamiteiten zoveel mogelijk te beperken dient er een continuïteitsplan te zijn dat er op gericht is de verstoring tot een aanvaardbaar niveau te beperken door een combinatie van preventieve maatregelen (voorkomen van verstoring) en herstelmaatregelen (het zo spoedig mogelijk hervatten van de essentiële verwerkingen).
De basis voor dit plan is wederom de risicoanalyse van de aanwezige verwerkingen waarbij voor elke klasse de maximaal toelaatbare onbeschikbaarheid wordt vastgesteld. Vanuit deze analyse worden stappen gedefinieerd die genomen moeten worden om de oorspronkelijke situatie te beschermen dan wel te herstellen. Dit plan moet procedures bevatten voor het veiligstellen, bewaren en terugzetten van gegevens (back-up in of buiten de plaats van de originele gegevens), uitwijkmogelijkheden voor essentiële apparatuur en afspraken met leveranciers van goederen en diensten die noodzakelijk zijn voor het functioneren van de systemen.
Alle onderdelen van het plan dienen op regelmatige basis in de praktijk te worden getest en geëvalueerd. De uitkomsten van deze testen moeten, conform de voorwaarden voor wijzigingsbeheer, opgenomen worden in de geldende continuïteit- en calamiteitenplannen. Uit deze eisen voor continuïteit[131] kunnen de volgende criteria worden gedestilleerd:

Criteria:
1. Is een proces ingericht voor het ontwikkelen en handhaven van de bedrijfscontinuïteit?
2. Is een risicoanalyse uitgevoerd waarbij gebeurtenissen zijn geïdentificeerd die de continuïteit van de bedrijfsprocessen in gevaar kunnen brengen en waarbij de gevolgen van onderbrekingen voor de bedrijfsprocessen zijn vastgesteld?
3. Zijn continuïteitsplannen opgesteld voor het in stand houden of herstellen van de bedrijfsactiviteiten na een onderbreking of verstoring van het bedrijfsproces?
4. Wordt (via SLA[132]) de beschikbaarheid van de netwerkinfrastructuur vastgelegd?
5. Zijn er voorzieningen getroffen om in geval van nood (brand, ontploffing) het netwerk beschikbaar te houden voor de aangeslotenen (b.v. via een uitwijklocatie en vervanging apparatuur)?
6. Worden continuïteitsplannen regelmatig getest, onderhouden en geëvalueerd?

6.6.11 Naleving

Alle hierboven genoemde eisen en uitgangspunten moeten duidelijk worden gespecificeerd en vastgelegd in procedures en werkinstructies welke inhoudelijk uiteraard in overeenstemming moeten zijn met geldende wettelijke regelingen en contractuele afspraken. Alle relevante documenten moeten worden beveiligd tegen verlies, vervalsing en vernietiging en worden opgenomen in een catalogus waarbij voor elk document de opslagplaats en –medium alsmede de geldigheids- en bewaartermijn worden geregistreerd.
De te beveiligen verwerkingen moeten in overeenstemming zijn met de overige eisen die de geldende privacywetgeving stelt, waarbij een volledig overzicht van aanwezige verwerkingen een eerste vereiste is. De organisatie moet op de hoogte zijn van de risico's van ongeautoriseerd gebruik van computers in het kader van de wet op de computercriminaliteit en mogelijke aansprakelijkheid bij misbruik van voorzieningen.
De verantwoordelijken voor verwerkingsprocessen moeten er dan ook voor zorgen dat geldende voorschriften worden nageleefd en regelmatig worden getoetst aan de geldende normen en, indien nodig, geactualiseerd. De volgende toetsingsvragen kunnen uit dit overzicht van nalevingseisen[133] worden vastgesteld:

[131] G.W van Blarkom, J.J. Borking, Beveiliging van persoonsgegevens, Den Haag, Registratiekamer, april 2001, pag. 49-51 en NEN 7510, Delft, Nederlands Normalisatie Instituut, april 2004, pag. 32-33.
[132] Service Level Agreement; diensten niveau overeenkomst.
[133] NEN 7510, Delft, Nederlands Normalisatie Instituut, april 2004, pag. 33-35.

Criteria:
1. Is binnen de organisatie bekend aan welke wetgeving, naast de WBP, allemaal voldaan moet worden?
2. Wordt binnen de organisatie periodiek beoordeeld dat conform relevante wetgeving gewerkt wordt?
3. Worden na een evaluatie de afspraken herzien en/of plannen gemaakt om e.e.a. aan te pakken en aan te scherpen?
4. Wordt een overzicht bijgehouden van de van toepassing zijnde wetten en contractuele voorschriften en de bijbehorende specifieke maatregelen en individuele verantwoordelijkheden?
5. Zijn maatregelen genomen om te waarborgen dat wordt voldaan aan wettelijke en contractuele vereisten met betrekking tot het gebruik van materiaal waarop intellectuele eigendomsrechten rusten?
6. Zijn maatregelen geïmplementeerd om belangrijke documenten en informatie tegen verlies, vernietiging en vervalsing te beveiligen en hiermee te voldoen aan wettelijke en zakelijke vereisten?
7. Zijn maatregelen getroffen om de naleving van privacywetgeving te waarborgen?
8. Zijn maatregelen genomen om ervoor te zorgen dat informatieverwerkende voorzieningen van de organisatie alleen voor geautoriseerde organisatiedoeleinden worden gebruikt?
9. Zijn procedures opgesteld om ervan verzekerd te zijn dat afspraken, wettelijke en contractuele vereisten met betrekking tot het gebruik van cryptografische middelen worden nagekomen?
10. Zijn regels aanwezig voor het verzamelen van bewijs dat kan worden gebruikt als ondersteuning bij een actie tegen een bepaalde persoon of organisatie?
11. Wordt regelmatig gecontroleerd en geëvalueerd of alle informatieverwerkende voorzieningen voldoen aan het beveiligingsbeleid, de beveiligingsnormen en andere beveiligingseisen?
12. Worden informatiesystemen regelmatig gecontroleerd op de naleving van technisch beveiligingsnormen?
13. Worden *audits* van operationele systemen gepland en goedgekeurd teneinde het risico van verstoringen van bedrijfsprocessen tot een minimum te beperken?
14. Wordt de toegang tot hulpmiddelen voor systeemaudits beheerd teneinde misbruik of verminking te voorkomen?

6.6.12 Beveiligingsincidenten

Verbeteringen in alle bovenstaande punten zijn pas mogelijk als ook alle incidenten en afwijkingen van de geldende procedures die ontdekt of vermoed worden, gerapporteerd worden aan de verantwoordelijke voor de beveiliging. Alle uitzonderingen op de normale gang van zaken en andere voorvallen die relevant zijn, moeten worden vastgelegd in logboeken. Dit is van toepassing op zowel uitzondering op systeemgebruik welke door gebruikers worden gemeld als ook op werkzaamheden van systeembeheerders. Deze logboeken moeten een registratie van de verstoring bevatten, de consequenties van deze verstoring voor de gegevensverwerking en de handelingen welke zijn uitgevoerd bij de afhandeling van de gerapporteerde storing. Deze registraties kunnen dienen als bewijsmateriaal en dus is het van belang dat de vastlegging geschiedt volgens geldende normen voor het verzamelen van bewijs en ook dat het verzamelde bewijs kwalitatief voldoende en volledig is. Alle gebruikers moeten ervan op de hoogte zijn dat gesignaleerde tekortkomingen in de beveiliging moeten worden gerapporteerd maar ook dat misbruik van een dergelijk beveiligingslek niet is toegestaan. De ontvangen meldingen moeten het begin vormen van een procedure voor afhandeling van beveiligingsincidenten, welke gericht is op evaluatie van de gemelde situatie en verbetering van de beveiliging. Uit deze eisen aangaande de afhandeling van beveiligingsincidenten[134] kunnen de volgende criteria worden afgeleid:

Criteria:
1. Is er een meldingsprocedure voor gebruikers voor beveiligingsincidenten?
2. Is er een registratieplicht voor systeembeheerders voor alle systeemwerkzaamheden en -verstoringen?
3. Bevatten de gevoerde registraties een overzicht van melding, consequenties en acties?
4. Is er een evaluatie- en verbeterproces voor gemelde incidenten?

[134] G.W van Blarkom, J.J. Borking, Beveiliging van persoonsgegevens, Den Haag, Registratiekamer, april 2001, pag. 33 en NEN 7510, Delft, Nederlands Normalisatie Instituut, april 2004, pag. 35-36.

6.7 Bewaartermijnen

Artikel 10 WBP introduceert de voorwaarde voor de bewaartermijn: persoonsgegevens mogen niet langer worden bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren dan noodzakelijk voor het bereiken van het doel waarvoor deze zijn verzameld. De verantwoordelijke dient zich af te vragen of er voldoende redenen zijn op grond waarvan de gegevens bewaard dienen te blijven. Zijn deze redenen aanwezig dan kan de verantwoordelijke bepalen welke bewaartermijnen op deze gegevens van toepassing zijn. Zijn deze redenen er niet, dan mogen de gegevens niet meer verwerkt worden tenzij voor een ander, verenigbaar doel. Voor bepaalde doeleinden geeft lid 2 een ruimere bewaartermijn.

Uit artikel 29 lid 2 blijkt dat bij AMvB termijnen kunnen worden vastgesteld gedurende welke persoonsgegevens mogen worden bewaard. In het Vrijstellingsbesluit zijn dan ook, als uitwerking van artikel 29, termijnen opgenomen waarbij de verantwoordelijke de verplichting heeft de persoonsgegevens voor het verstrijken van deze termijnen te verwijderen tenzij bewaren noodzakelijk is om te voldoen aan een andere wettelijke verplichting of bewaarplicht. Een eerste stap in deze afleiding is de controle of een verwerking onder het Vrijstellingbesluit valt. De meeste persoonsgegevens die worden verwerkt met betrekking tot personeel vallen onder artikel 7 Vb (maximaal 2 jaar na einde dienstverband). Administratieve gegevens van bewoners kunnen meestal onder artikel 17 Vb (5 jaar) of artikel 39 Vb (2 jaar) worden gebracht.

In gevallen die niet onder het Vrijstellingsbesluit vallen kunnen in bijzondere wetgeving nadere regels worden gesteld. Specifieke bepalingen over bewaartermijnen gaan voor op de algemene bepalingen uit de WBP. Op grond van het oude artikel 7:454 lid 3 BW moeten medische dossiers ten minste tien jaar bewaard blijven. De KNMG had instellingen al opgeroepen tot langer bewaren als dat ook maar enigszins juridisch mogelijk was. De Gezondheidsraad adviseerde zelfs een bewaartermijn van 30 jaar[135]. De Ministerraad heeft in december 2004 ingestemd met een wetsvoorstel waarbij de termijn verlengd wordt naar 15 jaar en de regering verwacht van instellingen dat deze hierop zullen anticiperen[136]. Inmiddels is het wetsvoorstel geaccepteerd waardoor de bewaartermijn van patiëntgegevens in de WGBO is verlengd naar 15 jaar[137].

De Wet BOPZ en het bijbehorende Besluit patiëntendossier BOPZ schrijven daarentegen voor dat opnamegegevens van gedwongen opgenomen psychiatrische patiënten vijf jaar moeten worden bewaard[138]. Andere wettelijke bepalingen gaan weer uit van vijftien jaar[139]. De formulering in de WBP en het feit dat specifieke bepalingen voorgaan op de algemene bepalingen uit de WBP heeft tot gevolg dat de concrete bewaartermijnen voor de verschillende verwerkingen uit specifieke wetten of regelingen moeten worden afgeleid. Met name sociale en fiscale wetgeving zal hier uitsluitsel moeten geven over de toegestane termijn. Het probleem hierbij kan zijn dat er verschillende termijnen worden gegeven door verschillende regelingen; sommige financieel-administratieve gegevens (verzekeringsgegevens) moeten volgens sociale wetgeving 5 jaar bewaard worden, volgens fiscale wetgeving 7 jaar terwijl het Vrijstellingsbesluit werkt met een termijn van 2 jaar[140]. Een instelling is dus verplicht alle verwerkingen feitelijk te toetsen op het specifieke karakter van de gegevens en de toepasselijke regelgeving. Voor wat betreft de dagelijkse praktijk resulteert dit in een verplichting om op welhaast continue basis de bestaande verwerkingen te controleren op inhoud en waar nodig op te schonen. De volgende toetsvragen zijn uit dit overzicht af te leiden:

---

[135] Gezondheidsraad, Bewaartermijn patiëntengegevens, Gezondheidsraad, Den Haag, 2004, publicatie nr. 2004/08, pag. 93.
[136] Persbericht van VWZ d.d. 10 december 2004, http://www.minvws.nl/persberichten/ibe/2004/wijziging-wet-beh-overeenkomst.asp
[137] Wijziging van enige bepalingen van het Burgerlijk Wetboek omtrent de overeenkomst inzake geneeskundige behandeling en van artikel IV van de wet van 17 november 1994, Stb. 837. Artikel I, onderdeel A, en artikel II treden in werking met ingang van 1 april 2005. Indien het Staatsblad waarin deze wet wordt geplaatst, wordt uitgegeven na 31 maart 2005, treden artikel I, onderdeel A, en artikel II in werking met ingang van de dag na de datum van uitgifte van het Staatsblad waarin deze wet wordt geplaatst, en werken deze artikelen terug tot en met 1 april 2005.
[138] Onder meer in artikel 23, artikel 56 lid 3 Wet BOPZ en artikel 2 lid 2 Besluit Patiëntendossier BOPZ
[139] J. Nouwt, Privacy en medische informatie in: J. Prins en J. Berkvens (red.), Privacyregulering in theorie en praktijk, Kluwer, Deventer, 2002, pag. 275.
[140] Helpdesk WBP / NVZ, overzicht persoonsgegevens, Utrecht, 2001

Criteria:

1. Is er voor de beschreven verwerking een (wettelijke) bewaartermijn vastgesteld?
2. Is de gehanteerde bewaartermijn in overeenstemming met de wettelijke regels?
3. Gelden afwijkende termijnen indien de gegevens in niet-herleidbare vorm worden bewaard?
4. Indien er geen wettelijke termijn is vastgesteld, is de gehanteerde bewaartermijn redelijk in combinatie met de voor deze verwerking gestelde doelen?

7 Ontwikkeling onderzoeksinstrument

7.1 Inleiding

In de voorgaande hoofdstukken is de theoretische basis gelegd voor inventarisatie en beoordeling van de verwerkingen binnen De Vitalis Zorg Groep. In dit hoofdstuk zal de vertaling worden gemaakt van deze theorie naar een handleiding voor het uitvoeren van inventarisatie en beoordeling in de concrete situatie: het interviewschema. Een interviewschema is meer dan slechts een lijst van mogelijk te stellen vragen; ook inleiding en introductie, antwoord- en noteersystemen en evaluatiecriteria maken deel uit van een gestructureerde aanpak van dataverzameling. Om te komen tot een goed interviewschema zullen een aantal stappen[141] worden doorlopen die, uitgaande van de oorspronkelijke onderzoeksvraagstelling en gebruikmakend van de informatie uit de voorgaande hoofdstukken, zullen leiden tot een praktisch bruikbare vragenlijst en instructies.

7.2 Stap 1: theoretische variabele

Het lijkt een open deur, maar interviews worden gehouden om een informatievraag te beantwoorden. De basisvraag die beantwoord zal moeten worden, is de onderzoeksvraag waarmee dit onderzoek is gestart:
Hoe krijgt de WBP zijn beslag binnen De Vitalis Zorg Groep en in hoeverre voldoet de organisatie aan de voorwaarden die door deze wet worden gesteld?

De verleiding is groot om op basis van deze startvraag een aantal interviewvragen te verzinnen, maar hierbij ontstaat het risico dat de verzameling losse vragen niet de gewenste informatie opleveren om de onderzoeksvraag te beantwoorden. Een eerste stap om dit risico te vermijden is het benoemen van theoretische variabelen of “ideale” variabelen die vooraf omschrijven welke informatie uit de interviews moet komen. De oplossing van dit probleem bestaat eruit dat er verzamelingen objecten worden gedefinieerd (A-verzameling) waarvan waarden en kenmerken worden verzameld die op de objecten van toepassing kunnen zijn (B-verzameling).
In dit onderzoek bestaat de A-verzameling van objecten uit de verwerkingen van persoonsgegevens binnen De Vitalis Zorg Groep. De B-verzameling, de verzamelingen van kenmerken van de objecten, bestaat uit de kenmerken zoals die in de voorgaande hoofdstukken zijn geïdentificeerd (verwerker, verantwoordelijke, melding, doel, betrokkenen, soort gegevens etc. etc.).
Schematisch ziet de uitwerking van de eerste stap er als volgt uit:

Nr.	Benaming	Verzameling A	Verzameling B
1	Welke verschillende verwerkingen zijn te onderscheiden?	Alle verwerkingen binnen Vitalis	Alle combinaties van begrippen uit hoofdstuk 3.
2	Voldoen de aanwezige verwerkingen aan de wettelijke eisen?	Alle verwerkingen binnen Vitalis	Alle combinaties van eisen aan verwerkingen uit hoofdstuk 4.

Tabel 1: overzicht theoretische variabelen

7.3 Stap 2: van theoretische naar ruwe variabelen

Met de lijst van theoretische variabelen uit de vorige stap wordt verder gewerkt. In stap 2 dienen te waarden uit de B-verzameling zodanig geconcretiseerd te worden dat er aan elk object uit de A-verzameling, een verwerking dus, steeds slechts één waarde uit de B-verzameling gekoppeld kan worden. Voor sommige variabelen kan dat eenvoudig zijn en kunnen de variabelen uit de B-verzameling direct in interviewvragen worden omgezet. In dit geval echter is dit niet mogelijk en moeten hulpvariabelen of indicatoren gezocht worden die wél in interviewvragen zijn om te zetten. De eis aan een hulpvariabele is dat deze zo veel samenhangt met de oorspronkelijke theoretische

[141] B. Emans, Interviewen, theorie, techniek en training, Groningen, Wolters-Noordhoff, 1990, pag. 101 e.v.; D.B. Baarda, M.P.M. de Goede, Methoden en technieken, Houten, Stenfert Kroese, 1995, pag. 141 e.v.

variabele dat deze voldoende wordt gerepresenteerd[142]. In dit onderzoek zijn de indicatoren zoals deze in hoofdstuk 5 en 6 zijn benoemd geschikt om als hulpvariabele te dienen.

Voor de theoretische variabele “welke verwerkingen zijn te onderscheiden” worden de begrippen uit hoofdstuk drie als ruwe variabelen gebruikt. In onderstaand schema wordt het een en ander verduidelijkt.

Nr.	Theoretische variabele	Indicator / ruwe variabele
1.1	Te onderscheiden verwerking	Contactpersoon / aanspreekpunt
1.2	Te onderscheiden verwerking	Naam van de verwerking en product of dienst waarvoor wordt verwerkt
1.3	Te onderscheiden verwerking	Doel en grondslag van de verwerking
1.4	Te onderscheiden verwerking	Betrokkene
1.5	Te onderscheiden verwerking	Categorieën van gegevens
1.6	Te onderscheiden verwerking	Bewerker
1.7	Te onderscheiden verwerking	Aan wie verstrekt
1.8	Te onderscheiden verwerking	Herkomst van de gegevens
1.9	Te onderscheiden verwerking	Toelichting op beveiliging
1.10	Te onderscheiden verwerking	Buitenlandse doorgiften
1.11	Te onderscheiden verwerking	Melding
1.12	Te onderscheiden verwerking	Omschrijving werking

Tabel 2: theoretische variabele 1 met bijbehorende indicatoren.

Voor de tweede theoretische variabele, voldoen aan de wettelijke eisen, moeten ook ruwe variabelen gezocht worden omdat de gewenste informatie niet direct uit één vraag kan worden verkregen. De begrippen uit hoofdstuk 6 zijn toepasbare indicatoren voor deze variabele. In het volgende schema is de overgang van de theoretische naar de ruwe variabele weergegeven.

Nr.	Theoretische variabele	Indicator / ruwe variabele
2.1	Voldoen aan wettelijke eisen	Transparantie
2.2	Voldoen aan wettelijke eisen	Doelbinding
2.3	Voldoen aan wettelijke eisen	Rechtmatige grondslag
2.4	Voldoen aan wettelijke eisen	Kwaliteit van gegevens
2.5	Voldoen aan wettelijke eisen	Beveiliging
2.6	Voldoen aan wettelijke eisen	Bewaartermijnen

Tabel 3: theoretische variabele 2 met bijbehorende indicatoren

7.4 Stap 3: detaillering van ruwe variabelen

De indicatoren die samen een beeld geven van de theoretische variabele zijn nu duidelijk, maar zelfs nu kunnen de gevonden ruwe variabelen niet direct in interviewvragen worden omgezet. Hiervoor is nog een gecombineerde stap nodig: detaillering en vraagindicering[143].
Het eerste deel dient ervoor om de ruwe variabelen verder uit te splitsen zodat die aspecten van de ruwe variabele die samen deze variabelen vormen concreet genoeg zijn om te dienen als basis voor een directe interviewvraag. Deze stap wordt ook wel detaillering van de ruwe variabele genoemd
Het tweede deel van deze stap, de indicering, geeft richting aan het soort vraag dat gesteld gaat worden. Het antwoord op een interviewvraag kan drie soorten informatie geven: feitelijke informatie, zelfbeschrijving van de respondent en gedragsintentie van de respondent. In het inventariserende deel van dit onderzoek wordt gevraagd naar de kenmerken van de actuele verwerkingen. Dit is een vraag naar feiten. Het type vraagstelling is hiermee gegeven.
Voor invulling van het eerste deel van deze stap, de verdere detaillering, moet teruggegrepen worden op de theoretische begrippen zoals die in hoofdstuk 3 en 4 zijn beschreven.

[142] B. Emans, Interviewen, theorie, techniek en training, Groningen, Wolters-Noordhoff, 1990, pag. 108.
[143] B. Emans, Interviewen, theorie, techniek en training, Groningen, Wolters-Noordhoff, 1990, pag. 109-111.

Voor de indicatoren van de eerste theoretische variabele is detaillering niet in alle gevallen noodzakelijk; de meeste indicatoren zijn dermate concreet dat direct een feitelijke vraag kan worden geformuleerd die de gewenste informatie geeft. De uitwerking voor de indicatoren van de eerste theoretische variabele in informatievragen is in onderstaande tabel uitgewerkt.

Nr.	Indicator / ruwe variabele	Informatievraag	Indicering
1.1	Contactpersoon / aanspreekpunt	Vragen naar functie of naam van diegene die in de dagelijkse praktijk de beheerder of het eerste aanspraakpunt is voor de verwerking.	Feitelijk
1.2	Naam en product of dienst	Vragen naar naam van de verwerking en product of dienst waarvoor de verwerking wordt uitgevoerd. Detaillering conform indeling in paragraaf 5.4 onder punt 2.	Feitelijk
1.3	Doel en grondslag	Vragen naar het doel van de verwerking en de wettelijke grondslag welke de basis vormt voor de verwerking. Detaillering conform grondslagen in artikel 8 WBP.	Feitelijk
1.4	Betrokkene	Vragen naar de betrokkene over wie gegevens worden verwerkt. Detaillering conform indeling in paragraaf 5.4 onder punt 4.	Feitelijk
1.5	Categorie van gegevens	Vragen naar welke gegevens worden verwerkt. Detaillering conform indeling paragraaf 5.4 onder punt 5.	Feitelijk
1.6	Bewerker	Vragen naar naam en functie van de partij die als bewerker gegevens verwerkt .	Feitelijk
1.7	Aan wie verstrekt	Vragen naar de namen of functies van de personen die gebruik maken van de verwerking. Detaillering conform indeling in paragraaf 5.4 onder punt 7.	Feitelijk
1.8	Herkomst	Vragen naar de oorsprong en de wijze van verkrijgen van de gegevens.	Feitelijk
1.9	Beveiliging	Vragen naar de maatregelen die genomen zijn ter beveiliging van deze verwerking.	Feitelijk
1.10	Buitenlandse doorgiften	Vragen naar eventuele buitenlandse verstrekkingen.	Feitelijk
1.11	Melding	Vragen naar ja/nee melding van deze verwerking.	Feitelijk
1.12	Werking	Vragen naar beschrijving van en toelichting op de werking van de genoemde verwerking.	Feitelijk

Tabel 4: informatievragen behorende bij theoretische variabele “te onderscheiden verwerking”.

Voor de indicatoren van de tweede theoretische variabele is het nog niet mogelijk directe vragen te formuleren; verdere detaillering is dus noodzakelijk. Voor deze detaillering wordt gebruik gemaakt van de criteria die bij de bespreking van de indicatoren in hoofdstuk 6 zijn afgeleid. Naast detaillering van de inhoudelijke vragen (de “IST”- vragen), dient per indicator ook het gewenste niveau vastgesteld te worden (de “SOLL”-vragen). Voor iedere indicator zal dus een inleidende vraag geformuleerd moeten worden die inzicht geeft in het ambitieniveau[144]. Bij het beschrijven van de verwerkingen wordt wederom gevraagd naar feiten, echter bij het beschrijven van het ambitieniveau wordt gevraagd naar een intentie van de respondent (hoe wilt u het hebben) in combinatie met een waardering van de huidige situatie. Voor het beschrijven van het ambitieniveau zal dus gebruikt gemaakt worden van een combinatie van vragen die zich richten op gedragsintentie en op zelfbeschrijving.

[144] Analoog aan de verdeling in de WBP- Zelfevaluatie. Zie G. van Blarkom, J. Leerentveld en R. Schreijnders (red.), WBP Zelfevaluatie, Den Haag, CBP, april 2001, pag. 7.

Nr.	Indicator / ruwe variabele	Detaillering en informatievraag	Indicering
2.1.0	Transparantie	Huidige situatie en ambitieniveau	Zelfbeschrijvend en gedragsintentie
2.1.1		Zijn de gegevens wel of niet rechtstreeks van betrokkene verkregen	Feitelijk
2.1.2		Kan informatie aan betrokkene achterwege blijven en zo ja: waarom	Feitelijk
2.1.3		Wanneer is betrokkene op de hoogte gesteld van de verwerking	Feitelijk
2.1.4		Welke informatie (doel, identiteit verantwoordelijke en/of aanvullende informatie) heeft betrokkene ontvangen?	Feitelijk
2.1.5		Is het voor betrokkene duidelijk hoe en waar een verzoek tot inzage moet worden ingediend?	Feitelijk
2.1.6		Zijn er termijnen afgesproken voor het geven van een reactie en zo ja, hoe lang zijn deze?	Feitelijk
2.1.7		Welke gegevens bevat een reactie op een verzoek tot inzage?	Feitelijk
2.1.8		Hoe kan een derde reageren op de voorgenomen informatieverstrekking naar betrokkene?	Feitelijk
2.1.9		Hoe is rekening gehouden met de volgende bijzondere omstandigheden: 1. Verzoek wordt niet schriftelijk ingediend? 2. Verzoek wordt niet door maar namens betrokkene ingediend?	Feitelijk
2.1.10		Hoe wordt de identiteit van verzoeker geverifieerd?	Feitelijk
2.1.11		Is het voor betrokkene duidelijk hoe en waar een verzoek tot wijziging moet worden ingediend?	Feitelijk
2.1.12		Is het duidelijk dat een verzoek tot wijziging slechts op drie manieren beantwoordt mag worden?	Feitelijk
2.1.13		Hoe worden wijzigingen doorgegeven aan derden?	Feitelijk
2.1.14		Is het voor betrokkene duidelijk hoe en waar een verzet moet worden ingediend?	Feitelijk
2.1.15		Is betrokkene gewezen op de mogelijkheid van absoluut verzet?	Feitelijk
2.1.16		Zijn er maatregelen getroffen om de verwerking terstond (bij absoluut verzet) dan wel na gerechtvaardigd relatief verzet, te beëindigen?	Feitelijk

Tabel 5: informatievragen behorende bij theoretische variabele “voldoen aan de wettelijke eisen”.

Op vergelijkbare wijze worden alle ruwe variabelen die behoren bij de theoretische variabele “voldoen aan de wettelijke eisen”[145] omgezet in de bijbehorende informatievragen met passende indicering. Het voert te ver om al deze afleidingen hier in detail uit te werken. De resultaten worden zichtbaar in de uiteindelijke interviewlijst die is opgenomen in bijlage 4. Om de hoofdlijn van deze methode van interviewontwerp zichtbaar te maken is voor de indicator “transparantie” de volgende stap uitgewerkt in paragraaf 7.6.2.

7.5 Stap 4: technische variabelen

In de stappen 2 en 3 zijn ruwe variabelen afgeleid vanuit de theoretische variabelen. Er is naast deze verzameling variabelen nog een andere categorie van ruwe variabelen die niet zijn afgeleid van de

[145] Doelbinding, Rechtmatige grondslag, Kwaliteit van gegevens, Beveiliging, Bewaartermijnen; zie Tabel 3

theoretische variabelen, maar die uit een andere bron komen[146]. Het gaat hierbij om de technische variabelen, nodig om de interviewresultaten te kunnen verwerken. Om welke variabelen het hierbij precies gaat is afhankelijk van de context waarbinnen het interview of de enquête plaatsvindt. Deze variabelen kunnen worden gebruikt om verderop in het onderzoek terug te kunnen grijpen op eenduidig te identificeren interviews, om verbanden te kunnen leggen tussen geïnterviewden en hun antwoorden of om, bijvoorbeeld bij onduidelijkheden of onvolledigheden in de antwoorden, de respondent te kunnen benaderen voor aanvullende informatie. Geheel binnen het gedachtegoed van de WBP zullen de gegevens die worden vastgelegd binnen de technische variabelen ter zake dienend, juist en volledig moeten zijn, zonder overmatig te worden.

Binnen dit onderzoek zullen, analoog aan de gegevens die het CBP vraagt van de contactpersoon, de volgende technische variabelen worden gebruikt:

Nr.	Indicator/ruwe variabele	Verzameling A	Verzameling B
T.1	Datum interview/ enquête	Alle interviews	De datum waarop interview is afgenomen
T.2	Naam respondent	Alle respondenten	Alle respondentnamen
T.3	Locatie / dienst	Alle respondenten	Locatienamen of stafdienstnamen waar de respondent werkzaam is

Tabel 6: technische variabelen

7.6 Stap 5: van ruwe variabele naar vragen, antwoord- en noteersystemen

In de voorgaande 4 stappen zijn de essentiële voorbereidingen getroffen om te komen tot een gestructureerd interview. Deze stap is niet meer dan een vertaling van de geformuleerde informatievragen in concrete interviewvragen en het opstellen van een zodanig interviewschema dat de respondent in staat is aan elke ruwe variabele, middels het beantwoorden van een concrete vraag, een specifieke waarde uit de oorspronkelijke B-verzameling toe te kennen[147]. Als eerste worden alle informatievragen op basis van de gekozen detaillering en indicering omgezet in directe interviewvragen.
Daarnaast zal voor elke vraag een waardenverzameling c.q. een set van antwoordmogelijkheden moeten worden vastgesteld die gezamenlijk de B-verzameling vormen. Deze vormen het antwoord- en noteersysteem. Binnen dit systeem wordt gekozen uit de mogelijkheden voor open vragen met dan wel zonder *fieldcoding* of gesloten vragen. Bij gesloten vragen krijgt de geïnterviewde een lijst met vaste alternatieve voorgelegd waaruit hij mag kiezen. Deze methodiek van vragen zal worden toegepast bij informatievragen waarbij het aantal antwoordmogelijkheden limitatief is vast te stellen. Open vragen zonder *fieldcoding* worden gebruikt als er geen vaste antwoordalternatieven zijn te benoemen of als dit aantal onevenredig groot dreigt te worden. De variant van open vragen met *fieldcoding* wordt alleen gebruikt in mondelinge interviews en is een tussenvorm waarbij aan de respondent een open vraag wordt gesteld, maar waarbij de interviewer uit een lijst met vaste alternatieven, onzichtbaar voor de geïnterviewde, het best passende alternatief als antwoord noteert. Ten slotte moeten, om de geïnterviewde door het interview te begeleiden, per vraag antwoordinstructies worden geformuleerd.

7.6.1 Uitwerking theoretische variabele 1: te onderscheiden verwerkingen

Toepassing van de methoden voor het afleiden van vragen, antwoord- en noteersystemen op de informatievragen die zijn afgeleid ten behoeve van de theoretische variabele “te onderscheiden verwerkingen” heeft onderstaande tabel tot resultaat.

Nr.	Indicator	Sub	Interviewvraag	Antwoordsysteem
1.1	Contactpersoon / aanspreekpunt		Wie is voor deze verwerking het eerstverantwoordelijke aanspreekpunt bij vragen?	Open vraag; Naam en functie noteren.

[146] B. Emans, Interviewen, theorie, techniek en training, Groningen, Wolters-Noordhoff, 1990, pag. 114.
[147] B. Emans, Interviewen, theorie, techniek en training, Groningen, Wolters-Noordhoff, 1990, pag. 116-121.

1.2	Naam en product of dienst	a	Hoe wordt deze verwerking in het dagelijks gebruik genoemd?	Open vraag; Naam van de verwerking noteren.
		b	Voor welke producten of diensten wordt deze verwerking gebruikt?	Gesloten vraag; kies een of meerdere van onderstaande alternatieven: Voor bewoners: o Persoonlijke verzorging, o Huishoudelijke verzorging, o Verpleging, o Ondersteunende begeleiding, o Activerende begeleiding, o Behandeling, o Verblijf Voor medewerkers: o Sollicitanten, o Uitzendkrachten, o Vrijwilligers, o Vast personeel, o Zieke werknemers, o Ex-werknemers, o OBU/gepensioneerden.
1.3	Doel en grondslag van de verwerking	a	Voor welk doel of welke samenhangende doelen worden deze gegevens verwerkt?	Open vraag; Doel van de verwerking noteren.
		b	Op welke (wettelijke) grondslag worden deze gegevens verwerkt?	Gesloten vraag; kies een of meerdere van onderstaande alternatieven: o De betrokkene heeft voor deze verwerking ondubbelzinnige toestemming gegeven, o De verwerking is noodzakelijk voor de nakoming van een (pre) contractuele verplichting die met betrokkene is of wordt aangegaan, o De verwerking is noodzakelijk omdat De Vitalis Zorg Groep hiertoe wettelijk verplicht is, o De gegevensverwerking is noodzakelijk omdat De Vitalis Zorg Groep hier een gerechtvaardigd belang bij heeft dat zwaarder weegt dan de privacy van de betrokkene.
1.4	Betrokkene		Over c.q. van wie worden in deze verwerking gegevens verwerkt?	Gesloten vraag; kies een of meerdere van onderstaande alternatieven: o Patiënt / bewoner, o Relatie van een patiënt / bewoner, o Externe hulpverlener, o Sollicitant, o Personeelslid, o Ziek of arbeidsongeschikt personeelslid, o Uitzendkracht c.q.

				gedetacheerde, ○ Vrijwilliger, ○ Ex-personeelslid, ○ Gepensioneerde / OBU, ○ Anders:
1.5	Categorie van gegevens		Welke categorieën c.q. soorten van gegevens zijn opgenomen in deze verwerking?	Gesloten vraag; kies een of meerdere van onderstaande alternatieven: ○ Persoonlijke of identificerende gegevens, ○ Financiële en administratieve gegevens, ○ Medische en sociaal-psychologische gegevens, ○ Gegevens met betrekking tot ras en etniciteit, ○ Gegevens met betrekking tot godsdienst en levensovertuiging, ○ Strafrechtelijke gegevens of gegevens die betrekking hebben op onrechtmatig dan wel hinderlijk gedrag, ○ Anders:
1.6	Bewerker		Worden verwerkingshandelingen door derden, buiten Vitalis, uitgevoerd?	Gesloten vraag; Kies een alternatief. ○ Nee ○ Ja Zo ja, door wie?
1.7	Aan wie verstrekt	a	Wie maakt er, naast uzelf, nog meer gebruik van de gegevens uit deze verwerking?	Open vraag; Functies of afdelingen of namen van gebruikers noteren.
		b	Wie heeft het dagelijks beheer over deze verzameling?	Open vraag; Functies of afdelingen of namen van beheerders noteren.
		c	Wie maakt er verder nog gebruik van de gegevens die in deze verwerking zijn opgenomen?	Open vraag; Functies of afdelingen of namen van derden noteren.
1.8	Herkomst		Van wie zijn de gegevens in deze verwerking verkregen?	Open vraag; Benoemen bronnen.
1.9	Beveiliging		Hoe zijn de gegevens uit deze verwerking beveiligd?	Open vraag; Korte omschrijving van genomen beveiligingsmaatregelen.
1.10	Buitenlandse doorgiften		Worden gegevens die in de verwerking zijn opgenomen doorgegeven aan buitenlandse gebruikers?	Gesloten vraag; Kies een alternatief. ○ Nee, ○ Ja, Zo ja: ○ Binnen de EU, ○ Buiten de EU, namelijk……
1.11	Melding		Is deze verwerking aangemeld?	Gesloten vraag, Kies een alternatief: ○ Nee, ○ Ja Zo ja, aangemeld bij ○ Functionaris Gegevensbescherming (FG) ○ College Bescherming

				Persoonsgegevens (CBP)
1.12	Werking		Geef een korte omschrijving van hoe deze verwerking werkt?	Open vraag; Beschrijf kort de werking.

Tabel 7: antwoord- en noteersysteem t.b.v. variabele 1

Met deze laatste stap is het inhoudelijke deel van het interview voor de inventarisatie compleet. De laatste stap is het samenvoegen van de gekozen technische variabelen en de uitgewerkte vragenlijst voor de eerste theoretische variabele en een geschikte lay-out te ontwerpen. Vanaf dit punt kan het complete inventarisatie-interview worden uitgezet in de organisatie. De uiteindelijke interviewlijst is opgenomen in bijlage 2. Het verloop van het inventarisatieproces en de ervaringen die hierbij zijn opgedaan zullen worden behandeld in het volgende hoofdstuk.

7.6.2 Uitwerking theoretische variabele 2: voldoen aan wettelijke eisen

Analoog aan de afleiding die in de vorige paragraaf is gebruikt om te komen tot een uitgewerkt vraag-, antwoord- en noteersysteem voor de theoretische variabele “te onderscheiden verwerkingen” is in onderstaande tabel het uiteindelijke interviewsysteem voor de tweede theoretische variabele “voldoen aan de wettelijke eisen” uitgewerkt. Ook hier is, met het oog op de leesbaarheid van dit verslag, de uitwerking bewust beperkt gehouden tot de indicator “transparantie”. De uiteindelijke resultaten zoals toepassing van deze stap oplevert voor de andere indicatoren, is terug te vinden in de uitgewerkte interviewschema’s in bijlage 4. De wijze waarop dit deel van het onderzoek in de organisatie is uitgevoerd, is onderwerp van het volgende hoofdstuk.

Nr.	Sub	Interviewvraag	Antwoordsysteem
2.1.0	a	Hoe beoordeelt u de huidige manier waarop de organisatie omgaat met de transparantie van gegevenverwerkingen en het informeren van de betrokkenen?	Gesloten vraag; Kies een van deze alternatieven: o Er zijn geen vastgelegde procedures en de verplichting tot informeren is niet in de organisatie bekend, o Er zijn geen vastgelegde procedures maar de verplichting tot informeren is in de organisatie bekend, o Er zijn geen vastgelegde procedures maar de betrokkenen worden consequent geïnformeerd, o Er zijn procedures vastgelegd en deze worden nageleefd, o Er zijn procedures vastgelegd welke worden nageleefd en waarvan de naleving periodiek wordt gecontroleerd.
	b	Wat is volgens u het streefniveau waarop de organisatie dient te komen voor wat betreft de transparantie van verwerkingen en het informeren van betrokkenen?	Gesloten vraag; Kies een van deze alternatieven: o Er zijn geen vastgelegde procedures en de verplichting tot informeren is niet in de organisatie bekend, o Er zijn geen vastgelegde procedures maar de verplichting tot informeren is in de organisatie bekend, o Er zijn geen vastgelegde procedures maar de betrokkenen worden consequent geïnformeerd, o Er zijn procedures vastgelegd en deze worden nageleefd, o Er zijn procedures vastgelegd welke worden nageleefd en waarvan de naleving periodiek wordt gecontroleerd.
2.1.1		Zijn de gegevens die in de verwerkingen zijn opgenomen	Gesloten vraag; Kies een van deze alternatieven:

		rechtstreeks van de betrokkene verkregen?	○ Ja ○ Nee
2.1.2		Kan informatieverstrekking over de kenmerken van de verwerkingen aan betrokkenen achterwege blijven?	Gesloten vraag; Kies een van deze alternatieven: ○ Nee, ○ Ja, want ○ De betrokkenen was al op de hoogte van het feit dat deze gegevens zijn opgenomen in een verwerking, ○ Het kost onevenredige inspanning om de betrokkenen te informeren over de verwerking, ○ De verwerking is voorgeschreven door de wet.
2.1.3		Wanneer is betrokkene geïnformeerd over de verwerking van zijn gegevens?	Gesloten vraag; Kies een van deze alternatieven: ○ Niet, ○ Op het moment dat betrokkene de gegevens verstrekte, ○ Vóór het moment dat de gegevens voor de eerste keer werden verwerkt, ○ Op het moment dat de gegevens voor de eerste keer werden opgenomen in een verwerking, ○ Anders, namelijk:.....
2.1.4		Welke informatie met betrekking tot verwerkingen heeft betrokkene ontvangen?	Gesloten vraag; Kies een of meerdere van deze alternatieven: ○ Doel van de verwerking, ○ Identiteit van de verantwoordelijke, ○ Anders, namelijk.....
2.1.5	a	Is het voor betrokkenen duidelijk waar c.q. bij wie een verzoek tot inzage in zijn gegevens moet worden ingediend?	Gesloten vraag; Kies een van deze alternatieven: ○ Ja, ○ Nee
	b	Is het voor betrokkenen duidelijk hoe een verzoek tot inzage in zijn gegevens moet worden ingediend?	Gesloten vraag; Kies een van deze alternatieven: ○ Ja, ○ Nee
2.1.6		Zijn er termijnen afgesproken waarbinnen een reactie op een verzoek van betrokkenen moet worden gegeven?	Gesloten vraag; Kies een van deze alternatieven: ○ Nee, ○ Ja, namelijk.....
2.1.7		Als gereageerd wordt op een verzoek tot inzage, welke gegevens bevat deze respons dan?	Open vraag, Omschrijf de inhoud van een reactie op een verzoek tot inzage.....
2.1.8		Hoe kan een derde, niet zijnde de betrokkene, reageren op een voorgenomen informatieverstrekking naar betrokkene?	Open vraag, Omschrijf de wijze waarop een derde zijn reactie kenbaar kan maken.....
2.1.9	a	Hoe wordt er omgegaan met een verzoek tot inzage dat niet schriftelijk wordt ingediend door betrokkene?	Open vraag, Omschrijf de wijze waarop met een niet-schriftelijk verzoek wordt omgegaan.....
	b	Hoe wordt er omgegaan met een verzoek tot inzage dat niet door maar namens betrokkene wordt ingediend?	Open vraag, Omschrijf de wijze waarop met een verzoek namens betrokkene wordt omgegaan.....

2.1.10		Hoe wordt de identiteit van een verzoeker geverifieerd?	Open vraag, Omschrijf de wijze waarop de identiteit van een indiener van een verzoek wordt geverifieerd.....
2.1.11	a	Is het voor betrokkenen duidelijk waar c.q. bij wie een verzoek tot wijziging van zijn gegevens moet worden ingediend?	Gesloten vraag; Kies een van deze alternatieven: ○ Ja, ○ Nee
	b	Is het voor betrokkenen duidelijk hoe een verzoek tot wijziging van zijn gegevens moet worden ingediend?	Gesloten vraag; Kies een van deze alternatieven: ○ Ja, ○ Nee
2.1.12		Op welke manieren wordt gereageerd op een verzoek tot wijziging?	Gesloten vraag; Kies een of meerdere van deze alternatieven: ○ Wijziging uitgevoerd, ○ Wijzigingsverzoek afgewezen, ○ Wijziging onmogelijk ○ Anders, namelijk.....
2.1.13		Hoe worden aangebrachte wijzigingen doorgegeven aan derden?	Open vraag, Omschrijf de wijze waarop wijzigingen in gegevens worden doorgegeven aan derden....
2.1.14	a	Is het voor betrokkenen duidelijk waar c.q. bij wie verzet moet worden ingediend?	Gesloten vraag; Kies een van deze alternatieven: ○ Ja, ○ Nee
	b	Is het voor betrokkenen duidelijk hoe verzet moet worden ingediend?	Gesloten vraag; Kies een van deze alternatieven: ○ Ja, ○ Nee
2.1.15		Is betrokkene gewezen op de mogelijk van absoluut verzet?	Gesloten vraag; Kies een van deze alternatieven: ○ Ja, ○ Nee
2.1.16		Indien er sprake is van absoluut verzet dan wel gerechtvaardigd relatief verzet, zijn er maatregelen getroffen om de verwerking terstond te beëindigen?	Gesloten vraag; Kies een van deze alternatieven: ○ Ja, ○ Nee

Tabel 8: antwoord- en noteersysteem t.b.v. variabele 2: voldoen aan de wettelijke eisen.

8 Uitvoering onderzoek

8.1 Inleiding

In het vorige hoofdstuk is de basis gelegd voor de uit te voeren deelonderzoeken: de inventarisatie van de verwerkingen en de toets op het naleven van de wettelijke eisen verdeeld in de quick-scan en de diepte-interviews. Gekozen is voor de dataverzamelingsweg van de interviews omdat de kernvragen uit het onderzoek gaan over attitude, opinie (hoe staat Vitalis tegenover de WBP, nu en in de toekomst) en kennis[148]. Een van de aandachtspunten bij het afnemen van interviews is de kleuring van de antwoorden als gevolg van sociale wenselijkheid, waardoor de validiteit van de gegevens negatief wordt beïnvloedt. Omdat bij mondelinge interviews het risico van sociale wenselijkheid kan worden beperkt door de rol van de interviewer is binnen dit onderzoek gekozen voor toepassing van beide vormen: schriftelijk voor de quick-scan en de inventarisatie en mondeling voor de detailinterviews die diep ingaan op de verschillende eisen die gesteld worden aan verwerkingen. Omdat de diepte-interviews in principe hetzelfde meten als de quick-scan kan een vergelijking tussen de uitkomsten een inzicht bieden in kleuring van de antwoorden.

Het toepassen van zowel mondelinge als schriftelijke interviews vraagt verschillende voorbereidingen. Schriftelijk interviewen vraagt veel aandacht voor de vragenlijst zelf, de lay-out en de leesbaarheid en de begrijpelijkheid van de vragen; tijdens het invullen is er voor de interviewer geen mogelijkheid meer om eventuele vragen van de respondent te beantwoorden. Een grondige proefafname van schriftelijke interviews is hierdoor noodzakelijk. Voor dit onderzoek impliceert dit dat voor zowel de quick-scan als voor de inventarisatie extra tijd is geïnvesteerd in zowel het uiterlijk en de begrijpelijkheid van de vragenlijst als ook in de proefafname. Regelmatige wijziging van vragen, begrippen en begeleidende teksten bleek noodzakelijk.
Gebruik van mondelinge interviews vraagt meer voorbereidingstijd van de interviewer zelf maar heeft als voordeel dat het beantwoorden van mondelinge vragen minder belastend is voor de respondenten waardoor meer en moeilijker vragen (zoals i.c. de vele en gedetailleerde vragen uit de diepte-interviews) beter beantwoord worden in face-to-face gesprekken.

Naast bovenstaande theoretische argumenten om te kiezen voor de genoemde interviewvarianten, speelt in deze fase van het onderzoek de voorkeur van de organisatie een belangrijke rol. Elk onderzoek kost tijd van de respondenten en het mag niet zo zijn dat deelname aan een onderzoek naar feiten die niet tot de kernactiviteiten van een zorgverlener behoren, de respondenten zal afleiden van het uitvoeren van de primaire zorgprocessen. Deze praktische beperking is er mede aanleiding toe geweest dat er bij de quick-scan en de inventarisatie voor schriftelijk interviewen is gekozen; bij de quick-scan is het tijdsbeslag minimaal en bij de inventarisatie van actieve verwerkingen kan op elk gewenst moment deelgenomen worden en hoeven niet alle verwerkingen in een keer beschreven te worden. Zelfs deze uitgangspunten konden niet voorkomen dat er van veel respondenten commentaar kwam op de belasting dit onderzoek vroeg.
Oorspronkelijk was het de bedoeling de beoordeling op het voldoen aan de wettelijke eisen samen met de beschrijving van de verschillende verwerkingen uit te voeren. Helaas bleek tijdens de theoretische fase van dit onderzoek dat zowel het aantal criteria waarop moet worden getoetst als ook de detaillering dermate groot waren, dat dit een ontoelaatbare belasting van de organisatie tot gevolg zou hebben indien elke operationele verwerking middels deze vragen zou worden getoetst. In overleg met de opdrachtgever(s) is toen besloten niet elke individuele verwerking te toetsen op de criteria zoals afgeleid in hoofdstuk 6 maar dit slechts op locatie c.q. stafdienstniveau te doen. In principe is hierdoor de eerste van de probleemstellingen in het gedrang gekomen, maar door rekening te houden met het gestelde in de onderzoekstelling (het ontwikkelde instrument moet geschikt zijn voor herhaalde toepassing) is er een systeem uitgekomen dat het mogelijk maakt om in de toekomst (en buiten het kader van dit afstudeeronderzoek) met dezelfde vragenlijst alle respondenten die hebben deelgenomen aan de inventarisatie van verwerkingen opnieuw te benaderen met een interview waarin de details van de wettelijk eisen aan verwerkingen worden beschreven.

Na de theoretische keuze voor interviewvormen en de praktische bijsturing van omvang en diepgang van de interviews zijn de definitieve vragenlijsten uitgewerkt en voorbereid voor de proefafname.

[148] D.B. Baarda, M.P.M. de Goede, Methoden en technieken, Houten, Stenfert Kroese, 1995, pag. 143 e.v.

8.2 Afname van interviews

8.2.1 Voorbereiding en uitvoering quick-scan

Zoals bij alle schriftelijke interviews, moet de gebruikte vragenlijst zowel qua inhoud als qua lay-out zo laagdrempelig mogelijk zijn en respondenten niet afschrikken. Vragen moeten duidelijk zijn en niet voor meer dan één uitleg vatbaar. Om dit te toetsen is het voor schriftelijke interviews noodzakelijk[149] een proefafname te houden op basis waarvan de vragenlijst bijgesteld en definitief gemaakt kan worden.
Uitgangspunt bij de omzetting van de vragen die zijn afgeleid in paragraaf 7.6.2 (theoretische variabele “voldoen aan de wettelijke eisen”) was de noodzaak tot een tweedeling van de vragenlijsten in een quick-scan en een diepte-interview. Deze tweedeling was gebaseerd op de wens van de organisatie om de invloed op de werkprocessen zo laag mogelijk te houden. Als eerste schriftelijk interview is dan ook de quick-scan in de organisatie uitgezet. De eerste proefafname is gedaan met de vragen die betrekking hebben op de huidige situatie en het ambitieniveau, in dezelfde vorm als in het vorige hoofdstuk afgeleid. Met gebruikmaking van de beschikbare techniek binnen Vitalis zijn de vragen opgenomen in een elektronische lijst die via het intranet aan de respondenten werd aangeboden. Hierdoor is bereikt dat gewenste aanpassingen snel en direct zichtbaar voor respondenten konden worden uitgevoerd, waardoor er in de uitvoeringfase weinig tijd voor onderhoud van de lijsten nodig was. De voorbereiding hiervoor vroeg daardoor wel veel tijd omdat alle vragen ingevoerd moesten worden in de hiervoor gebruikte “formuliermodule” van het content-managementsysteem van Vitalis[150]. Het resultaat is, nog voordat de eerste proefafname is gehouden, doorgesproken met de opdrachtgever. Op basis van zijn opmerkingen is de terminologie van de vragen aangepast en versimpeld. Hierna is de vragenlijst gepubliceerd op het Intranet en is de link naar de pagina verspreid onder de medewerkers van de locatie[151] die deelnam aan de proefafname.
Uit de evaluatie van de resultaten (zowel inhoudelijk als qua lay-out en techniek) bleek dat wederom aanpassingen noodzakelijk waren. Technische aanpassingen hadden o.m. betrekking op de gewenste mogelijkheid van de respondenten om feedback te krijgen van hun antwoorden hetgeen middels een e-mail constructie is gerealiseerd. De gewenste aanpassingen aan inhoud waren wederom gericht op de complexiteit van de gebruikte terminologie, het abstractieniveau van de vragen en onduidelijkheid over de begrippen privacy, betrokkene, verwerking enz. Hoewel de verzoeken om aanpassing niet inhoudelijk getoetst of geëvalueerd zijn, was het aantal verzoeken wel een indicatie voor de onbekendheid met de begrippen uit de WBP en de toepassing van het privacybegrip in de vorm van informationele privacy. Na aanpassing van de vragenlijst is de enquête opnieuw gepubliceerd op het intranet en zijn de andere locaties en stafdiensten per e-mail uitgenodigd om deel te nemen aan de quick-scan. Ook nu kwamen er nog vragen van respondenten die aanpassingen in de vorm van het toevoegen van voorbeelden en het nog verder toelichten van wettelijke termen noodzakelijk maakten. Waar nodig zijn de respondenten in persoon ondersteund bij het toelichten en invullen van de enquête. Hiermee is enerzijds de doorlooptijd verlengd maar de kwaliteit van de ingediende data is hiermee omhoog gegaan. De uiteindelijke resultaten van dit deel van de enquête worden verder besproken in paragraaf 9.1.

8.2.2 Voorbereiding en uitvoering inventarisatie van verwerkingen

De voorbereidingen van dit deel van het onderzoek verliepen analoog aan de voorbereidingen van de quick-scan. Ook hier zijn de vragen uit paragraaf 7.6.1 ingevoerd in het content-managementsysteem en doorgesproken met de opdrachtgever. Noodzakelijke aanpassingen hadden ook bij dit deel van het onderzoek betrekking op het versimpelen van vraagstellingen, het toevoegen van verklarende teksten, het uitbreiden van de definities en voorzien van voorbeelden. Ook de feedback tijdens de proefafnames was hierop gericht. Het aantal initiële reacties dat als melding werden geretourneerd was laag. Hieruit bleek o.m. dat het begrip “verwerking” erg eng werd uitgelegd door de respondenten en dat bij “betrokkene” in de meeste gevallen slechts aan bewoners/cliënten werd gedacht. Ook hier bleek dat de kennis van de begrippen en de invloed daarvan op de dagelijkse praktijk laag was. Door het toevoegen van voorbeelden is de reikwijdte van de begrippen verder toegelicht. Na deze

[149] D.B. Baarda, M.P.M. de Goede, Methoden en technieken, Houten, Stenfert Kroese, 1995, pag. 145
[150] met dank aan mijn collega’s van de afdeling ICT voor de korte cursus “Mambo” en “Phil-a-form” en de ondersteuning bij het programmeren van de systemen en databases.
[151] Woonzorgcentrum Theresia, directie dhr. N. Van Dongen.

aanpassingen zijn de overige locaties en ondersteunende diensten per e-mail uitgenodigd deel te nemen aan dit deel van het onderzoek. Zelfs tijdens de onderzoeksfase zijn nog kleine aanpassingen in de teksten van de vragenlijst uitgevoerd, met name gericht op het detailleren van toelichtingen en het uitbreiden van de voorbeelden. Ook woordkeus en zinsbouw van de vragen zijn versimpeld. Daarnaast zijn bij de inventarisatie een aantal respondenten in één-op-één sessies persoonlijk begeleid bij het invullen van de meldingsformulieren.

8.2.3 Voorbereiding en uitvoering diepte-interviews

Zoals reeds eerder aangegeven was het de bedoeling alle aanwezige verwerkingen te toetsen op de criteria uit hoofdstuk 6 hetgeen in de praktijk zou neerkomen op het toepassen van ongeveer tweehonderd vragen, verdeeld over de zes benoemde ruwe variabelen. Dit zou voor de organisatie een te grote belasting zijn en er tevens toe leiden dat de doorlooptijd van dit onderzoek veel te lang zou worden. In overleg met de opdrachtgever is er voor gekozen de detailtoets uit te voeren op locatieniveau en voorlopig niet per geïdentificeerde verwerking. Dit had wel tot gevolg dat een ander scoringssysteem moest worden gekozen voor die vragen die specifiek op benoemde verwerkingen van toepassing zijn.
Er is voor gekozen een uitspraak te laten doen over de stand van zaken voor alle verwerkingen geaggregeerd, hetgeen resulteerde in een 5-punts schaal van

- nooit; waarde 2,
- soms (minder dan 50% van de gevallen); waarde 3,
- meestal (meer dan 50% van de gevallen) ; waarde 4,
- altijd; waarde 5

met daarnaast uiteraard de keuzemogelijkheid “weet niet” (waarde 1) indien de status van de verwerkingen niet bekend is (hetgeen overigens direct een indicatie is voor de mate waarin de WBP leeft)[152]. In sommige gevallen was het niet mogelijk een vraag te formuleren die beantwoord kon worden over alle verwerkingen heen[153]. De toets op het betreffende criterium is niet opgenomen in de huidige vragenlijst, maar blijft voor het vervolgonderzoek (het toetsen van de individuele verwerkingen) uiteraard wel relevant. De hiervan afgeleide vragenlijsten zijn opgenomen in bijlage 4.

[152] Analoog aan de vragenlijsten die het NEN ter beschikking stelt als handreiking bij de invoering van de NEN-7510 in netwerkorganisaties. Hiermee is voorkomen dat binnen dit onderzoek opnieuw het wiel wordt uitgevonden en is bereikt dat de gebruikte methode aansluit bij de standaard die door auditoren wordt gebruikt. De resultaten van dit onderzoek kunnen dan ook in de toekomst vergeleken worden met uitkomsten van onderzoeken bij andere organisaties.
[153] Bijvoorbeeld de vraag “van wie zijn de gegevens verkregen”. Indien deze vraag wordt gesteld met als doelgebied alle verwerkingen, is het antwoord nietszeggend immers alle antwoordmogelijkheden zullen bij deze vraagstelling voor kunnen komen.

9 Analyse onderzoeksgegevens

9.1 Quick-scan

Doel van de quick-scan was om een snel en compact overzicht te geven van huidige situatie en het ambitieniveau van de organisatie voor wat betreft het voldoen aan de eisen uit de WBP. Per locatie dient hiervoor een score per onderdeel[154] alsmede een totaalscore voor huidige situatie en ambitieniveau te worden vastgesteld. Om de locaties onderling te vergelijken dienen de uitkomsten per indicator te worden genormaliseerd. Omdat er hier sprake is van nominale gegevens[155], wordt de mediaan als waarde voor de onderlinge vergelijking gebruikt. De zekerheid waarmee kan worden vastgesteld of de gevonden mediaan representatief is voor de locatie (en voor de organisatie als geheel) is uiteraard afhankelijk van het aantal ingevulde enquêtes. Om een uitspraak te kunnen doen over de mate waarin de gevonden waarde is te generaliseren naar de totale populatie (per locatie of voor Vitalis als geheel) moet de schattingsfout worden berekend[156]. Voor wat betreft de individuele locaties is het aantal ingevulde enquêtes te laag om als basis voor verdere analyse te dienen. Voor Vitalis als geheel ligt de schattingsfout binnen de afrondingsgrenzen van de naast-hogere of lagere schaal (zie bijlage 7). De gevonden waarden mogen dus gegeneraliseerd worden naar de totale populatie.

De bedoeling is om middels de uitkomsten van de quick-scan tot een totaalscore te komen voor wat betreft de variabele “voldoen aan de eisen” met betrekking tot de huidige situatie en het ambitieniveau van Vitalis. Om te komen tot een totaalscore worden de uitkomsten per indicator (i.c. zes, te weten transparantie, doelbinding etc. etc.) bij elkaar opgeteld om te komen tot een totaalwaarde[157] voor “huidige situatie” en “ambitieniveau”. Als voor een samengestelde variabele (zoals hier “huidige situatie”) meer dan één indicator wordt gebruikt, moet echter eerst met behulp van een itemanalyse of correlatietoets getoetst worden of de antwoorden op alle zes de indicatoren hetzelfde begrip meten[158]. Om te concluderen dat de verschillende indicatoren inderdaad hetzelfde meten wordt hiervoor de homogeniteitsindex (Alpha) berekend over alle vragen en de correlatie tussen de antwoorden op telkens 2 verschillende antwoorden[159].
Het blijkt dat bij de huidige situatie slechts vraag 1 en 3 een Alpha van minder dan 0,2 hebben. Alle vragen samen correleren op 0,86 (maximaal 0,88 indien vraag 3 niet wordt meegenomen). Deze waarde geeft aan dat de individuele vragen inderdaad dezelfde begrippen meten en dat de waarden van de verschillende vragen met betrekking tot de huidige situatie mogen worden samengevoegd in één variabele. Voor de vragen die betrekking hebben op de gewenste situatie blijkt de Alpha 0,88 te zijn en lager te worden indien vragen worden weggelaten. Ook hier kunnen de uitkomsten van de individuele vragen worden samengevoegd tot één nieuwe variabele (zie bijlage 7).
De beoordeling van de huidige situatie komt hiermee op “2” (geen procedures, maar de begrippen zijn wel bekend echter worden niet nageleefd) en de beoordeling van de gewenste situatie komt hiermee op “4” (wel vastgelegde en nageleefde procedures echter nog geen toetsing op naleving hiervan). Voor wat betreft de huidige situatie geeft de organisatie dus zelf al aan dat niet wordt voldaan aan de WBP omdat de beginselen weliswaar bekend zijn in de organisatie maar niet worden nageleefd.

Voor de keuze welke maatregelen moeten worden genomen en waar deze maatregelen als eerste toegepast moeten worden is het van belang te analyseren of er verschillen zijn in huidige situatie en ambitieniveau tussen de locaties onderling en tussen de locaties en de Vitalis-score. Op deze manier kan worden vastgesteld binnen welke locatie moet worden begonnen (de laagste score op “huidige situatie” c.q. de hoogste score op “ambitieniveau”) en op welk gebied moet worden gestart

[154] transparantie, doelbinding, rechtmatige grondslag, kwaliteit van gegevens, beveiliging, bewaartermijnen
[155] Bij een ordinale verdeling krijgen de eigenschappen niet een willekeurige waarde maar geeft de schaal een rangorde weer. Een hogere waarde op de schaal geeft aan dat een eigenschap groter, langer, belangrijker etc. is. Er wordt slechts gemeten of een eigenschap meer of minder voorkomt, niet in welke mate een eigenschap meer of minder voorkomt. E. Huizing, Inleiding SPSS, Schoonhoven, Academic Services, 1999, pag. 21.
[156] D.B. Baarda, M.P.M. de Goede, Methoden en technieken, Houten, Stenfert Kroese, 1995, pag. 217; SPSS: Analyze -> Descriptive statistics -> Frequencies.
[157] Een normale berekening van het rekenkundig gemiddelde: (huidige situatie transparantie + huidige situatie doelbinding + ….+ huidige situatie bewaartermijn)/6. Analoog voor de berekening van de gewenste situatie c.q. het ambitieniveau.
[158] D.B. Baarda, M.P.M. de Goede, Methoden en technieken, Houten, Stenfert Kroese, 1995, pag. 203;
[159] Beide toetsen worden via de functie “RELIABILITY” binnen SPSS tegelijk uitgevoerd. Alpha kan in waarde variëren van 0 tot 1, waarbij de waarde 1 aangeeft dat de vragen elkaar volledig overlappen. Correlatie moet minstens 0,20 zijn om te kunnen concluderen dat de vragen hetzelfde meten. SPSS: Analyze -> Scale -> Reliability

(transparantie etc.). Binnen de statistische terminologie is hier de locatienaam de (nominale) onafhankelijke- of splitsingsvariabele en de score op “huidige situatie” en “ambitieniveau” de (ordinale) afhankelijke variabele[160]. De toets is of de gevonden waarden statistisch significante verschillen laten zien tussen de locaties onderling, echter het probleem hierbij is dat er sprake is van ordinale variabelen en er dus geen gemiddelde scores kunnen worden gebruikt. Om alsnog tot onderbouwde conclusies te komen over de mate van verschil moet worden getoetst middels rangorde-scoring[161]. Uitgangspunt bij deze analyse is dat er per locatie een “steekproef” is getrokken en dat getoetst wordt of de waarden die per steekproef gevonden zijn significant verschillen tussen de locaties. Uit de uitgevoerde testen blijkt geen significant verschil in de antwoorden tussen de verschillende locaties. Hierdoor hoeft geen onderscheid gemaakt te worden in de aandachtspunten per locatie, maar kan verder gewerkt worden met de geaggregeerde uitkomsten voor de gehele organisatie. Conclusies en aanbevelingen kunnen dan ook voor alle deelnemende locaties gezamenlijk gegeven worden.

9.2 Diepte-interviews “voldoen aan wettelijke eisen”

Het oorspronkelijke doel van deze vragenlijst was de toets op het al dan niet voldoen aan de wettelijke eisen, uitgevoerd per beschreven verwerking. Zoals reeds eerder aangegeven is de uitvoering door praktische beperkingen vanuit de onderzoeksomgeving gewijzigd; de toets heeft niet plaats gevonden per verwerking maar per organisatieonderdeel.

De statistische voorbereidingen zijn analoog aan die welke zijn uitgevoerd bij de quick-scan. Om te komen tot een uitspraak over de in paragraaf 7.3 benoemde theoretische variabele c.q. de afgeleide ruwe variabelen wordt in principe de weg die is gevolgd bij de afleiding naar interviewvragen in omgekeerde richting afgelegd. Eerst is op de antwoorden van de, bij de verschillende indicatoren behorende, detailvragen de itemanalyse uitgevoerd (zie bijlage 8: correlatietoetsen). Van de uitkomsten van de detailvragen is, per indicator, de mediaan bepaald waarmee inzicht is verkregen in de stand van zaken met betrekking tot de indicator transparantie voor zowel ICT als de rest van de organisatie, voor wat betreft de stand van zaken met betrekking tot doelbinding, etc. etc. (zie bijlage 8: uitkomsten per indicator).

De laatste verwerkingsstap is het samenvoegen van de uitkomsten per indicator tot een einduitkomst voor de theoretische variabele “voldoen aan de WBP”. Ook hier is eerst getest op significante verschillen in de uitkomsten van de ICT afdeling ten opzichte van de rest van de organisatie met behulp van een rangordetoets[162], zowel voor wat betreft de 6 indicatoren apart als voor wat betreft de eindresultaten voor de theoretische variabele “voldoet aan de WBP” (zie bijlage 8: non parametric tests) . Het blijkt dat er bij de uitkomsten voor de individuele indicatoren slechts bij “bewaartermijnen” een significant verschil zit in de mate waarin de ICT-afdeling voldoet aan de WBP t.o.v. de rest van de organisatie. Bij het toetsen van de samengevoegde waarden voor de theoretische variabele blijkt er geen significant verschil te zijn tussen ICT en de rest van de organisatie. Alle waarden mogen dus worden beschouwd als zijnde afkomstig uit één populatie waardoor de actiepunten in gelijke mate geldend zijn voor zowel de afdeling ICT als voor de rest van de organisatie. De eindwaarde van de theoretische variabele bedraagt, teruggebracht naar de complete organisatie (dus zowel ICT als de rest) een “3” ofwel, in de terminologie van de achterliggende vragenlijst, De Vitalis Zorg Groep voldoet soms aan de WBP.

Statistics

VOLDOET

N	Valid	9
	Missing	0
Median		3,0000

[160] D.B. Baarda, M.P.M. de Goede, Methoden en technieken, Houten, Stenfert Kroese, 1995, pag. 223.
[161] Kruskal-Wallis-test of mediaan-test voor onafhankelijke steekproeven. D.B. Baarda, M.P.M. de Goede, Methoden en technieken, Houten, Stenfert Kroese, 1995, pag. 224-225. E. Huizingh, SPSS 9 voor Windows, Schoonhoven, Academic Services, 1999, pag. 353 e.v . ; SPSS: Analyze -> Non-parameteric tests -> K independent samples
[162] Omdat er hier sprake is van slechts twee groepen kan hier een Mann-Whitney-toets of een Kolmogorov-Smirnov-toets worden uitgevoerd i.p.v. de Kruskall-Wallis-toets of de Median-toets uit de vorige paragraaf, waar sprake was van meer dan twee groepen. Zie E. Huizingh, SPSS 9 voor Windows, Schoonhoven, Academic Services, 1999, pag. 350 e.v.
SPSS: Analyze -> Non-parameteric tests -> 2 independent samples. Voor de statistici: er wordt hier getoetst op de 0-hypothese dat er geen significant verschil is in de uitkomsten van de afdeling ICT t.o.v. de rest van de organisatie.

10 Conclusies en aanbevelingen

10.1 Conclusies

10.1.1 Algemeen

Terugkijkend naar het uitgangspunt van dit onderzoek en de vraag waarmee ooit is gestart (voldoet Vitalis aan de WBP?), moet er nu geconcludeerd worden dat dit eigenlijk een vraag is die niet beantwoord kan worden.
De WBP, ooit tot stand gebracht omdat er volgens de regering behoefte was aan specifieke, bovensectorale, privacywetgeving ter bescherming van de informationele privacy, is ontworpen als een “omnibuswet”, ingevuld met vage normen en ruime definities[163]. Om te komen tot een bruikbare invulling van deze wet moet een beroep gedaan worden op een veelheid van andere regelingen, sectorale regels, beleidsafspraken, grondrechten etc. Voor verantwoordelijke en betrokkenen in dit onderzoek blijkt de WBP als beschermingsinstrument van informationele privacy dan ook nauwelijks te leven, laat staan actief toegepast te worden, omdat het voor de gemiddelde organisatie zonder specialistische hulp gewoonweg onmogelijk is de WBP als direct ijkpunt voor privacybescherming te gebruiken.
De vraag of een organisatie i.c. De Vitalis Zorg Groep, aan de eisen van de WBP voldoet kan dus beter anders geformuleerd worden: voldoet de organisatie aan de algemene privacybeginselen zoals deze in verschillende wettelijke regelingen zijn uitgewerkt? De WBP kan hier slechts de rol van startpunt vervullen, maar draagt niet of nauwelijks bij aan de invulling.

Is de WBP hiermee verworden tot dode letter? Wellicht wel en ook kan privacybescherming wellicht beter worden gerealiseerd door niet uit te gaan van specifieke privacywetgeving in de vorm van de WBP maar door gebruik te maken van bestaande wetgeving zoals het BW[164]. Toch heeft het abstracte karakter van de WBP en het hierin gehanteerde toestemmingsbeginsel geleid tot een zekere standaardisatie van het beschermingsregime en een checklist voor verwerking. Weliswaar moet er een (onpraktische) veelheid aan andere regelingen worden gebruikt om de begrippen uit de WBP te vertalen naar de praktijk, maar het voordeel hiervan is wel dat de WBP bruikbaar is voor verschillende technologieën van gegevensverwerking. Juist de ruime definities en de vage normen waarvoor de WBP wordt bekritiseerd, maken deze wet in feite technologie onafhankelijk waardoor deze niet per definitie onbruikbaar wordt als er nieuwe verwerkingsmethoden worden geïntroduceerd.

Zal De Vitalis Zorg Groep ooit aan de WBP voldoen? Nee, en wel om drie redenen.
Ten eerste is er de dynamiek van de huidige organisatie; beleid verandert, de dagelijkse behoefte aan meer of andere verwerkingen wijzigt van dag tot dag, meldingen zoals die zijn geïnventariseerd op basis van de uitgangspunten in hoofdstuk 5 veranderen qua inhoud of doel, kortom de verwerkingen wijzigen constant en zullen dus steeds opnieuw getoetst en (indien van toepassing) gemeld moeten worden.
Ten tweede zijn er de veranderingen in techniek, in organisatie, in communicatie met betrokkenen, in doelen voor verwerking kortom alle deelgebieden uit hoofdstuk 6 waardoor “voldoen aan de eisen van de WBP” een continue toetsing, evaluatie en bijsturing zal vereisen.
Als laatste is er de problematiek van de terminologie van de WBP. Door het gebruik van open normen kan een organisatie niet zelf vaststellen of er aan de WBP is voldaan. Slechts een (rechterlijke) toetsing achteraf zal antwoord kunnen geven of er een aanvaardbare afweging heeft plaatsgevonden tussen de belangen van de betrokkene en de belangen van de organisatie. Een (bestuurs-)rechterlijke toets op de algemene beginselen van behoorlijk bestuur (in verticale verhoudingen) of op de zorgvuldigheid die in het maatschappelijke verkeer is vereist[165] (in horizontale verhoudingen) geeft voor één specifieke verwerking in één specifieke context uitsluitsel over het al dan niet voldoen aan de eisen die de WBP stelt. Voor alle niet getoetste situaties kan een organisatie niet meer dan zijn uiterste best doen in de hoop dat de uitgevoerde acties een juiste vertaling van de WBP zijn.

[163] De basis voor de WBP, de Richtlijn, omvat 72 overwegingen en 34 artikelen. De WBP zelf omvat 83 artikelen welke worden toegelicht in een memorie van toelichting van 200 pagina’s.
[164] C. Cuijpers, Privacy of privaatrecht, een privaatrechtelijk alternatief voor de implementatie van de Europese privacyrichtlijn, Den Haag, SDU, 2004.
[165] H.J.J. Leenen, Handboek gezondheidsrecht deel 1: rechten van mensen in de gezondheidszorg, Houten, Bohn Stafleu van Loghum, 2000, pag. 270.

10.1.2 Uit het onderzoek: kwalitatief

Uit de vragen die ontstonden als reactie op de quick-scan en de inventarisatie blijkt dat de begrippen “informationele privacy” en de WBP inhoudelijk vrijwel onbekend zijn in de organisatie; ruimtelijke privacy wordt meestal als enige indicator van het privacybegrip herkend. Begrippen leiden tot verwarring en worden verkeerd uitgelegd of ten onrechte gescheiden zoals persoonsgegevens van bewoners en van medewerkers. Hoewel de meeste reacties op het onderzoek als zodanig positief waren, werd de naleving van de achterliggende regelgeving gezien als “extra werk” en als additionele administratieve belasting welke de aandacht afleidt van datgene waar het bij Vitalis werkelijk om gaat: de zorg. Het valt niet te ontkennen dat naleving van de WBP in het algemeen en deelname aan een onderzoek als dit in het bijzonder, een grote inspanning van de organisatie vraagt die ten koste kan gaan van andere werkzaamheden, maar de geconstateerde lage respons herbergt een groot risico voor de verantwoordelijke. Het is immers de plicht van de verantwoordelijke zorg te dragen voor eenduidige melding van de verwerkingen en de hierop volgende verdere naleving van de WBP[166].
De onbekendheid is mede een gevolg van het feit dat informationele privacy als begrip niet of nauwelijks voorkomt op de agenda van beleidspunten en hierdoor ook niet of nauwelijks zal indalen in de operationele werkzaamheden. Het risico dat privacybewustzijn en het naleven van de WBP als “vreemde activiteiten” beschouwd worden en niet als onderdeel van het dagelijkse werk is daardoor groot.

10.1.3 Uit het onderzoek: kwantitatief

Statistisch gezien is de respons onvoldoende om met zekerheid conclusies te formuleren. Het risico van de lage respons en de mogelijke oorzaken hiervan zijn in de vorige paragraaf al aan de orde geweest. Om in de toekomst toch voort te kunnen bouwen zijn de voorgenomen statistische analyses alsnog uitgevoerd als ware er voldoende grondslag. De organisatie als geheel blijkt qua naleving van de WBP geen vastgelegde procedures te hebben en waar de begrippen als zodanig bekend zijn, worden deze niet consequent nageleefd in de dagelijkse werkzaamheden; Vitalis voldoet “soms” aan de WBP. Ten opzichte van de huidige situatie legt de organisatie de lat wel hoog voor wat betreft de ambities: procedures zijn vastgelegd en worden nageleefd.
Specifiek binnen de ICT-afdeling blijkt de technische naleving van de NEN-7510 wel te gebeuren, maar het formele beleidsmatige en procedurele kader ontbreekt. De keuzes die gemaakt zijn en worden, zijn gebaseerd op technische uitgangspunten en zijn niet per definitie slecht, maar missen de aansluiting met de rest van de organisatie, met name op het gebied van het herkennen van de noodzaak van de uitgevoerde acties.

10.2 Aanbevelingen

10.2.1 Algemeen

Dit onderzoek beslaat zowel een stuk theorie als een stuk praktische toepassing van het positief recht. Vanuit de juridische theorie kan er kritiek geleverd worden op de WBP, maar vanuit de praktijk kan de WBP blijven zoals hij is. Praktisch gezien is de WBP een bruikbaar startpunt voor toepassing in de dagelijkse praktijk. Uiteenrafelen van deze wet en de onderdelen onderbrengen bij andere wetten zoals het BW zal in de praktijk nog meer verwarring veroorzaken. Juist om te komen tot eenduidige uitwerking van de privacybeginselen is verdere bundeling van de nu nog in andere wetgeving zwervende bepalingen een goede volgende stap.

10.2.2 Voor de organisatie

Op dit moment voldoet organisatie niet aan de WBP en de kennis van de WBP is onvoldoende om direct met concrete acties gericht op naleving te starten. Er zal een fundament van begrip gelegd moeten worden door eerst bewustwording te kweken. Door aandacht voor privacy-awareness in de organisatie moeten de medewerkers zich bewust worden van de verplichtingen die op hen rusten en de consequenties van niet nakoming. Deze awareness zal via verschillende wegen bereikt moeten worden. Als eerste moeten informationele privacy en informatiebeveiliging deel laten uitmaken van standaard managementcyclus en zal de kennis van de WBP top-down de organisatie in gebracht

[166] H.J.J. Leenen, Handboek gezondheidsrecht deel 1: rechten van mensen in de gezondheidszorg, Houten, Bohn Stafleu van Loghum, 2000, pag. 252.

moeten worden. Daarnaast zal op de werkvloer het begrip voor informationele privacy verhoogd moeten worden door op een toegankelijke manier en zonder al te veel formeel taalgebruik kennismakingsbijeenkomsten te organiseren[167].
Het beschrijven en melden van de individuele verwerkingen kan op dit moment niet de hoogste prioriteit krijgen omdat de kennis die nodig is om verwerkingen te “herkennen” onvoldoende is. Pas als de awareness-cyclus is doorlopen kan opnieuw gestart worden met de inventarisatie. De quick-scan als meetmiddel blijft wel actueel en zeker geschikt voor herhaalde toepassing. Als de organisatie de basiskennis heeft over de inhoud en de consequenties van de WBP kan de quick-scan opnieuw worden afgenomen, zowel bij dezelfde set respondenten als binnen dit onderzoek maar ook op lagere niveaus in de organisatie. Aandachtspunt bij een nieuwe afname zal wel de “verplichting tot deelname” moeten zijn om te voorkomen dat, net als binnen dit onderzoek, de respons onvoldoende is. Vergelijking van de huidige resultaten met die van toekomstig afnamen kunnen een duidelijk beeld geven van de behaalde resultaten maar ook van de nog uit te voeren acties.
Praktische punten die op korte termijn geïmplementeerd kunnen worden zijn: duidelijke informatie voor alle nieuwe medewerkers tijdens de bestaande introductiebijeenkomsten over nut en noodzaak van bescherming van informationele privacy, opstellen van gedragsregels voor clean desk regels, meer aandacht voor de rol van de functionaris gegevensbescherming. Daarnaast zal de reeds gegeven presentatie met betrekking tot informationele privacy op alle locaties en voor alle managementlagen gegeven moeten worden.

10.2.3 Gericht tot ICT

Gezien de toekomstige toetsingen zoals die o.m. door de IGZ zijn aangekondigd, kan de aanbeveling voor de ICT-afdeling kort zijn: zorg voor eenduidige implementatie van de NEN-7510. Deze aanbeveling is natuurlijk in de praktijk te breed om verder mee te kunnen. Ook hier zal privacy-awareness een eerste aandachtspunt moeten zijn zodat ook binnen deze afdeling het wettelijk kader van privacybescherming duidelijk wordt. Gezien de huidige stand van de techniek, zijn een aantal maatregelen al voldoende, maar ontbreekt het kader. De weg naar de NEN-7510 zal dan ook vanuit twee kanten tegelijk bewandeld moeten worden. Aan de ene kant zal een beleidsmatige basis gelegd moeten worden waarop de afdeling toekomstige acties kan baseren en zal dit beleid onderdeel moeten worden van de informatie die de afdeling krijgt (top-down). Aan de andere kant mag de techniek niet afwachten totdat het beleid duidelijk is; technische hulpmiddelen voor privacybescherming (zoals PET en encryptie) zoals deze door de markt worden aangeboden zullen individueel op hun waarde voor de systemen moeten worden beoordeeld en waar nodig ingevoerd (bottom-up). Deze beide wegen moeten in de nabije toekomst (een á twee jaar) convergeren zodat een integraal systeem van beleid en techniek ontstaat. Controle door een externe partij op naleving van de NEN-7510 en andere wettelijke bepalingen en een eventuele certificering zal zeker moeten gebeuren.
Praktische punten die op korte termijn geïmplementeerd kunnen worden zijn het beschrijven van bestaande werkwijzen in procedures, aanscherpen van het reeds geldende protocol voor e-mail en internetgebruik, het aanpassen van de procedures voor het toelaten van nieuwe gebruikers op het netwerk en het vaststellen van bewaartermijnen voor de verwerkingen van de afdeling ICT conform de bepalingen in het Vrijstellingsbesluit.

De huidige enquêteformulieren, zoals deze op het Intranet beschikbaar zijn gesteld, moeten actief blijven. Hierdoor wordt bereikt dat de organisatieonderdelen waarbinnen de bewustwording toeneemt direct met evaluatie en melding aan de slag kunnen, waardoor dit een continu proces kan worden. Indien het draagvlak voor de WBP voldoende is toegenomen en het naleven van de wet als integraal deel van de werkzaamheden wordt gezien (en niet meer als extra belasting) kan het meldingsformulier worden uitgebreid met de toetsingcriteria zoals deze binnen dit onderzoek nog zijn opgenomen in de vragenlijst voor de diepte interviews. De bestaande vragenlijst zal hiervoor wel ingekort moeten worden.

[167] Een proefsessie op de locatie Theresia leidde al vrij snel tot een heel andere kijk op privacy en de WBP als ook praktische acties over hoe bestaande verwerkingen aangepast konden worden.

Bijlage 1: geraadpleegde bronnen

Literatuur

1. Artz, S.M., en L.E. van Laviere, *De Wet bescherming persoonsgegevens, over de bescherming van uw persoonlijke gegevens,*
   Den Haag, CBP, 2002.

2. Baarda, D.B. en M.P.M. de Goede, *Methoden en technieken*,
   Houten, Stenfert Kroese, 1995.

3. Blarkom, G. van en J.J. Borking, *Beveiliging van persoonsgegevens*,
   Registratiekamer, Den Haag, 2001.

4. Blarkom, G. van, J. Leerentveld en R. Schreijnders (red.), *Raamwerk privacy audit,*
   Den Haag, CBP, april 2001.

5. Brouwer, J.G., *Compendium Wet bescherming persoonsgegevens, tekst en toelichting,*
   Den Haag, Koninklijke Vermande, 2002.

6. CBP, *Overgangsrecht WBP,*
   Den Haag, CBP, 2001.

7. Crebas, E.M. et al (red.), Reikwijd*te WBP in: Handboek Privacy in de gezondheidszorg,*
   Den Haag, Koninklijke Vermande, 2002.

8. Cuijpers, C., *Privacy of privaatrecht, een privaatrechtelijk alternatief voor de implementatie van de Europese privacyrichtlijn,*
   Den Haag, SDU, 2004.

9. Emans, B., *Interviewen, theorie, techniek en training*,
   Groningen, Wolters-Noordhoff, 1990.

10. Gezondheidsraad, *Bewaartermijn patiëntengegevens*,
    Den Haag, Gezondheidsraad, 2004, publicatie nr. 2004/08

11. Holvast, J., *Wet bescherming persoonsgegevens: overzicht en stappenplan,*
    Privacy & Informatie, 1998, nr. 1.

12. Hooghiemstra, T.F.M., *Privacy bij ICT in de Zorg. Bescherming van persoonsgegevens in de informatiestructuur van de gezondheidszorg,*
    Den Haag, CBP, 2002.

13. Hooghiemstra, T.F.M., *Tekst en toelichting Wet bescherming persoonsgegevens*,
    Den Haag, Koninklijke Vermande, 2003.

14. Huizingh, E., *Inleiding SPSS 9.0 voor Windows en Data Entry,*
    Schoonhoven, Academic Service, 1999.

15. Leenen, H.J.J., *Handboek gezondheidsrecht deel 1: rechten van mensen in de gezondheidszorg*,
    Houten, Bohn Stafleu van Loghum, 2000.

16. NEN 7510, *Informatiebeveiliging in de zorg,*
    Delft, Nederlands Normalisatie Instituut, april 2004

17. Nouwt, J., *Zorg voor privacy, informatietechnologie en informationele privacy in de gezondheidszorg,*
Den Haag, SDU, 1997.

18. Nouwt, J., *WBP: veranderingen voor de zorgsector,*
in: Privacy en Informatie, 2000, nr. 3(2)

19. Nouwt, J. en C. Louwerse, *Algemene beginselen van gegevensverwerking, in: Handboek privacy in de zorg,*
Den Haag, Koninklijke Vermande, 2004.

20. Prins, J. en J. Berkvens (red.), *Privacyregulering in theorie en praktijk,*
Deventer, Kluwer, 2002,

21. Rijkers, D., *Privacy, De Wet Bescherming Persoonsgegevens,*
Alphen aan den Rijn, Adformatie Groep, 2002.

22. Sauerwein, L.B. en J.J. Linneman, *Handleiding voor verwerkers van persoonsgegevens,*
Den Haag, Ministerie van Justitie, 2001.

23. VOG, *WBP, Handleiding bij het invoeren van de wet bescherming persoonsgegevens,*
Utrecht, VOG, 2001.

24. Wieringa, P. en M. van den Toorn (red.), *Jaaroverzicht Zorg in: Handboek Privacy in de gezondheidszorg,*
Den Haag, Koninklijke Vermande, 2004.

25. Witmer, J.M. en R.P. de Roode (red.), *Van wet naar praktijk. Implementatie van de WGBO. Deel 2,*
KNMG, Utrecht, 2004.

Internet

1. http://www.cbpweb.nl/bis/content-1-14-12.html
2. http://rechten.uvt.nl/sjaaknouwt/Zorgvisi.doc; Invoering van de WBP in tien stappen
3. http://www.minvws.nl/persberichten/ibe/2004/wijziging-wet-beh-overeenkomst.asp
4. http://www.grondweteuropa.nl/9326000/1/j9vvgjnazrhmix9/vgm7mnouggz9

Bijlage 2: uitgewerkt interviewschema t.b.v. inventarisatie verwerkingen.

De Vitalis Zorg Groep is, zoals alle organisaties die persoonlijke gegevens beheren en/of verwerken, verplicht zich te houden aan de Wet Bescherming Persoonsgegevens (WBP) en andere privacyregels. Deze wet geeft aan wat de rechten zijn van iemand van wie gegevens worden gebruikt en wat de verplichtingen zijn van organisaties die gegevens gebruiken. Verzamelen en verwerken van persoonsgegevens moet gebeuren binnen de voorwaarden en verplichtingen zoals gegeven in de wet. Deze voorwaarden hebben o.a. betrekking op het in kaart brengen van de verwerkingen en de doelen, de waarborgen om onnodige verzameling of onjuist gebruik van gegevens te voorkomen. Daarnaast moet een klacht- en inzagerecht gewaarborgd zijn.

Om inzicht te krijgen in hoeverre onze organisatie voldoet aan de eisen die de WBP stelt, eisen die in 2005 gecontroleerd gaan worden door de IGZ, wordt een onderzoek uitgevoerd binnen Vitalis. Dit onderzoek bestaat uit 3 delen: een inventarisatie van alle actieve gegevensverwerkingen binnen de gehele Vitalis Zorg Groep, een quick-scan om een overzicht te krijgen van de stand van zaken met betrekking tot de globale eisen van de WBP en een aantal diepte-interviews waarbij op detailniveau wordt gekeken naar de wijze waarop Vitalis zich conformeert aan de WBP.

Deze enquête is de inventarisatie. De bedoeling van dit deel van het onderzoek is alle verwerkingen (lees: gegevensverzamelingen) die op dit moment binnen De Vitalis Zorg Groep worden gebruikt, te inventariseren en de kenmerken ervan in kaart te brengen. Een afgeleide bonus van deze inventarisatie is dat na dit onderzoek alle actieve verwerkingen zijn vastgelegd en dat is nou net een van de eisen die binnen de komende controle door de IGZ wordt gesteld.

Het is de bedoeling dat u voor elke aparte gegevensverwerking waar u gebruik van gemaakt of waar u bij betrokken bent, telkens één formulier invult. Per vraag worden de gebruikte begrippen toegelicht en wordt een korte invulinstructie gegeven.

De gegevens die u verstrekt zullen anoniem worden verwerkt, dat wil zeggen dat alleen de onderzoekers inzage hebben in uw persoonlijke gegevens. De resultaten zullen anoniem worden gepresenteerd aan de Raad van Bestuur en samenvattingen worden verstuurd naar de directies en hoofden ondersteunende diensten.

Mocht u nog vragen hebben, neem dan gerust contact op met S. van der Pol (s.vander.pol@vitalis-zorggroep.nl), telefoon: 040-2933526

Alvast dank voor uw medewerking.

Introductie begrippen uit de Wet Bescherming Persoonsgegevens

Persoonsgegevens.

Gegevens zijn persoonsgegevens als deze gegevens informatie bevatten over een natuurlijke persoon en die persoon identificeerbaar is. Identificeerbaar is deze persoon uiteraard als er een naam wordt opgeslagen, maar ook andere gegevens die het mogelijk maken achter deze naam te komen vallen het begrip "persoonsgegevens". Voorbeelden hiervan zijn een telefoonnummer, het kenteken van een auto, een kamernummer, sofi-nummer, kortom alle gegevens waarmee je achter de identiteit van de persoon over wie het gaat kunt komen. De WBP noemt de persoon van wie persoonsgegevens verwerkt worden "de betrokkene".

In de praktijk kunnen dit gegevens zijn van zowel bewoners, medewerkers, vrijwilligers, externe hulpverleners of combinaties hiervan in de vorm van adreslijstjes, maaltijdregistraties, adresgegevens van bewoners of relaties van bewoners, de e-mailadressen zoals die op het netwerk staan, een overzicht van de welzijnsmeldingen enz. enz.

Verwerkingen.

Een gegevensverwerking is het hele proces dat een persoonsgegeven doormaakt, vanaf het moment dat het wordt verkregen tot en met het moment dat het wordt vernietigd (een samenhangend geheel van handelingen binnen één totaal computerprogramma bijvoorbeeld de salarisadministratie of de bewonersadministratie).

Daarnaast valt ook elke afzonderlijke technische- of verwerkingshandeling onder het begrip "verwerking" (verwerking in de enkelvoudige betekenis zoals opslaan, kopieren, mailen of printen).

Voor deze inventarisatie betekent dit dat alle (computer)bestanden en programma's die binnen Vitalis in gebruik zijn onder het begrip verwerking vallen en dat deze meegenomen moeten worden in de beoordeling, behalve de uitzonderingen die hieronder worden beschreven.

Uitzonderingen die niet beschreven hoeven te worden.

De wet is niet van toepassing op verwerkingen voor persoonlijk of huishoudelijk gebruik. Onder deze uitzondering vallen o.a. persoonlijke aantekeningen of adresbestanden die slechts door één persoon en voor zichzelf worden gebruikt. Deze behoeven dus niet te worden meegenomen in deze inventarisatie.

Uw naam:

Uw lokatie of dienst:

Identificerende gegevens m.b.t. beschreven verwerking
Niet alleen voor betrokkenen is het van belang te weten bij wie vragen kunnen worden gesteld over de beschreven verwerking maar ook voor het duidelijk herkennen van de verschillende gegevensverwerkingen binnen dit onderzoek .

Vraag 1.1
Wie is voor deze beschreven verwerking het eerste aanspreekpunt bij vragen; gelieve naam en functie te noteren van degene bij wie vragen gesteld kunnen worden.

Om tijdens de uitwerking van het onderzoek verwerkingen te kunnen vergelijken en te categoriseren maar ook om tijdens verdere interviews ervoor te zorgen dat het duidelijk is over welke verwerking wordt gesproken, moet de beschreven verwerking eenduidig zijn benoemd.

Vraag 1.2.a
Hoe wordt deze verwerking in het dagelijks gebruik genoemd (b.v. bestellijst maaltijden, presentielijst aanwezigheidsmelding, verzuimregistratie etc.)?

Vraag 1.2.b
Voor welk product of welke dienst wordt deze verwerking gebruikt?

Voor bewoners: persoonlijke verzorging,

Voor bewoners: huishoudelijke verzorging

Voor bewoners: verpleging

Voor bewoners: ondersteunende begeleiding

Voor bewoners: activerende begeleiding

Voor bewoners: behandeling

Voor bewoners: verblijf

☐

Voor medewerkers: sollicitanten

☐

Voor medewerkers: uitzendkrachten

☐

Voor medewerkers: vrijwilligers

☐

Voor medewerkers: vast personeel

☐

Voor medewerkers: zieke werknemers

☐

Voor medewerkers: ex-werknemers

☐

Voor medewerkers: OBU-Gepensioneerden

☐

Doel en grondslag van de verwerking
Het uitgangspunt van de Nederlandse privacywetgeving is dat alle handelingen met persoonsgegevens in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze moeten gebeuren. De wet gebruikt hiervoor de begrippen “doelbinding” en “grondslag”.

Doelbinding betekent dat gegevens alleen maar mogen worden verwerkt ten behoeve van vooraf uitdrukkelijk omschreven en gerechtvaardigde doelen. De verzamelde gegevens mogen ook niet worden gebruikt voor doeleinden die niet met het oorspronkelijke doel verenigbaar zijn. Om dit te kunnen beoordelen is het van belang dat u zo duidelijk mogelijk omschrijft voor welk doel de gegevens in deze verwerking worden gebruikt.

Naast doelbinding stelt de wet ook de eis dat er een rechtmatige grondslag moet zijn voor de verwerking. Dit betekent dat persoonsgegevens alleen mogen worden verzameld en verwerkt wanneer de grondslag hiervoor in de wet kan worden gevonden.

Vraag 1.3a
Wat is het doel of doelen van deze verwerking; graag zo nauwkeurig mogelijk beschrijven waarom deze gegevens worden verwerkt en wat hiermee bereikt moet worden?

[ ] *

Vraag 1.3b
Op basis van welke wettelijke grondslag worden deze gegevens verwerkt; een of meer van onderstaande alternatieven aankruisen?

De betrokkene heeft voor deze verwerking ondubbelzinnige toestemming gegeven en er is dus geen twijfel mogelijk dat betrokkene het eens is met de verwerking.

☐

De verwerking is noodzakelijk voor de nakoming van een (pre)contractuele verplichting die met betrokkene is of wordt aangegaan en De Vitalis Zorg Groep kan deze verplichting alleen maar nakomen door deze gegevens te verzamelen en te verwerken.

☐

De verwerking is noodzakelijk omdat een andere wet dan de WBP De Vitalis Zorg Groep verplicht om deze gegevens te verwerken.

☐

De gegevensverwerking is noodzakelijk omdat De Vitalis Zorg Groep hier een belang bij heeft dat zwaarder weegt dan de privacy van de betrokkene.

☐

Betrokkenen
Bij de inleiding op deze inventarisatie is al aangegeven dat met begrip betrokkene wordt bedoeld “de direct of indirect identificeerbare persoon van wie persoonsgegevens worden verwerkt”. Binnen een verwerking moet het duidelijk zijn over wie / van wie gegevens zijn vastgelegd en dat hoeft niet persé van één persoon te zijn.

Vraag 1.4
Over wie c.q. van wie worden in deze verwerking persoonsgegevens verwerkt; een of meer alternatieven aankruisen?

Gegevens over patiënt of bewoner

☐

Gegevens over relaties van patiënt of bewoner

☐

Gegevens over externe hulpverleners (buiten Vitalis)

☐

Gegevens over sollicitanten

☐

Gegevens over vast personeel (niet ziek of arbeidsongeschikt)

☐

Gegevens over zieke of arbeidsongeschikte personeelsleden

☐

Gegevens over uitzendkrachten, inleners en gedetacheerden

☐

Gegevens over (actieve) vrijwilligers

☐

Gegevens over ex-personeelsleden (niet leeftijdgebonden)

☐

Gegevens over gepensioneerden en OBU

☐

Andere typen betrokkenen voor zover niet hierboven genoemd:

Soorten persoonsgegevens
Het begrip persoonsgegevens is een ruim begrip waar veel verschillende categorieën van gegevens onder vallen. Al deze categorieën vallen onder verschillende wettelijke regelingen voor wat betreft eisen en voorwaarden voor verwerking. Om de geïnventariseerde verwerkingen te kunnen beoordelen is het dus noodzakelijk precies te weten welke soorten persoonsgegevens in deze verwerking zijn opgenomen.

Vraag 1.5
Welke categorieën c.q. soorten van gegevens zijn opgenomen in deze verwerking; kies een of meerdere van onderstaande alternatieven.

Persoonlijke en/of identificerende gegevens

☐

Financiële en administratieve gegevens

☐

Medische en sociaal-psychologische gegevens

☐

Gegevens met betrekking tot ras en etniciteit

☐

Gegevens met betrekking tot godsdienst en levensovertuiging

☐

Strafrechtelijke gegevens of gegevens die betrekking hebben op onrechtmatig dan wel hinderlijk gedrag

☐

Andere soorten of categorieën van gegevens voor zover niet hierboven benoemd:

Bewerker
De mogelijkheid bestaat dat bepaalde verwerkingen van gegevens buiten de organisatie plaatsvinden, door derden in opdracht van De Vitalis Zorg Groep. Om te voorkomen dat door deze constructie bepaalde verantwoordelijkheden kunnen worden ontdoken introduceert de WBP het begrip “bewerker”. Een bewerker verwerkt persoonsgegevens op last van de verantwoordelijke zonder aan diens rechtstreeks gezag te zijn onderworpen. Een voorbeeld van een bewerker is een bedrijf dat voor de instelling de salarisadministratie voert. De derde, de bewerker, heeft geen zeggenschap over de verwerking, maar handelt volgens de instructies en onder verantwoordelijkheid van de verantwoordelijke.

Vraag 1.6
Worden op deze verzameling persoonsgegevens verwerkingshandelingen uitgevoerd door derden, buiten De Vitalis Zorg Groep? Kies één van onderstaande alternatieven.

○ Nee
○ Ja

Zo ja, wie is voor deze verzameling de bewerker?

Ontvangers
De WBP verstaat hieronder degene aan wie persoonsgegevens worden verstrekt, binnen of buiten de eigen organisatie. Dit begrip is erg ruim; er vallen niet alleen personen, afdelingen of instanties onder die van anderen persoonsgegevens krijgen aangeleverd, maar ook personen die op basis van hun functie een of andere vorm van toegang hebben tot de gegevensverwerkingen. Het begrip “ontvanger” wordt verdeeld in drie categorieën:

Gebruiker
Een gebruiker hoeft niet noodzakelijkerwijs een individu te zijn, maar kan ook een groep of een afdeling zijn. In tegenstelling tot de bewerker (zie vorige vraag) staat de gebruiker wel onder gezag van de verantwoordelijke.

Beheerder
Naast de verantwoordelijke is het van belang te weten wie er de dagelijkse zorg voor de verwerkingen heeft. Meestal zal dit een afdelingshoofd of een groepsleider zijn. Per verwerking is er meestal maar één beheerder, maar een organisatie kan dus meerdere beheerders voor verschillende verwerkingen hebben.

Derde(n)
Deze restcategorie omvat allen die, niet zijnde betrokkenen, verantwoordelijken, bewerkers of enig ander persoon onder rechtstreeks gezag van de verantwoordelijke of de bewerker, gemachtigd zijn persoonsgegevens te verwerken.

Vraag 1.7a
Wie maakt er, naast uzelf, nog meer gebruik van de gegevens uit deze verwerking? Functies, afdelingen of gebruikersnamen opgeven a.u.b.

Vraag 1.7b
Wie heeft het dagelijks beheer over deze verwerking? S.v.p. functie, afdeling of beheerdersnaam opgeven.

Vraag 1.7c
Wie maakt er verder nog gebruik van de gegevens uit deze verwerking, voor zover nog niet benoemd in de vorige vragen? Functies, afdelingen of gebruikersnamen opgeven a.u.b.

Herkomst gegevens
Het beschrijven van de herkomst van de verwerkte gegevens is van belang omdat deze consequenties heeft voor de meldingsplicht van de organisatie. Daarnaast is er een verband tussen bron van de gegevens en de toegestane doelen van deze verwerking.

Vraag 1.8
Van wie zijn de gegevens die in deze verwerking zijn opgenomen verkregen c.q. afkomstig; benoem de verschillende bronnen zoals bijvoorbeeld de betrokkene zelf, andere personen of organisaties of andere verwerkingen?

Beveiliging
Beveiligingsmaatregelen kunnen in drie soorten worden onderscheiden. Ten eerste vallen daar de geheimhoudingsplichten onder op grond van beroep, ambt, wettelijk voorschrift of contract. Een tweede beveiligingsmaatregel betreft het nemen van passende technische en organisatorische maatregelen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Ten derde is De Vitalis Zorg Groep ook verantwoordelijk voor de deugdelijkheid van de beveiligingsmaatregelen die de bewerker neemt. Beveiliging is een onderdeel dat op detailniveau ook verderop in het onderzoek ter sprake zal komen. Bij deze vraag volstaat het kort te beschrijven welke beveiligingsmaatregelen specifiek op deze verwerking van toepassing zijn.

Vraag 1.9
Hoe zijn de gegevens uit deze verwerking beveiligd; geef a.u.b. een korte omschrijving van de genomen maatregelen?

Buitenlandse doorgiften
Het is toegestaan om medische hulp in het buitenland te zoeken voor bijvoorbeeld een bril, tandheelkundige hulp of zelfs (hart)transplantaties. Uiteraard zal zich in deze gevallen de noodzaak voordoen van uitwisseling van (medische) persoonsgegevens met het buitenland. Binnen de EU is dit geen probleem, maar persoonsgegevens mogen in principe slechts doorgegeven worden naar landen buiten de EU indien deze een voldoende niveau van bescherming garanderen.

Vraag 1.10
Worden gegevens die in deze verwerking zijn opgenomen doorgegeven aan buitenlandse gebruikers; kies één van onderstaande alternatieven?

- (•) Geen doorgifte van gegevens uit deze verwerking aan het buitenland
- ( ) Gegevens uit deze verwerking gaan naar landen binnen de EU
- ( ) Gegevens uit deze verwerking gaan naar landen buiten de EU

Melding
Formeel moet elke verwerking van persoonsgegevens zijn aangemeld bij het College Bescherming Persoonsgegevens (CBP) in Den Haag of bij de Functionaris Gegevensbescherming (FG) in onze organisatie. Het spreekt voor zich dat afzonderlijke aanmelding van alle mogelijke gegevensverwerkingen zal leiden tot een administratieve overbelasting van het CBP. Om dit te voorkomen zijn door de WBP veel vrijstellingen van deze meldingsplicht gegeven. Het gaat bij deze verwerkingen om allerlei standaardregistraties die worden omschreven in het Vrijstellingsbesluit. Vrijstelling van melding mag alleen indien de verwerking voldoet aan de voorwaarden uit het Vrijstellingsbesluit. Om te voldoen aan de eisen uit de meldingsplicht is het van belang per geïnventariseerde verwerking te weten of en zo ja bij wie deze is aangemeld.

Vraag 1.11
Is deze verwerking aangemeld; kies een van onderstaande alternatieven?

- (•) Niet gemeld
- ( ) Aangemeld bij de functionaris gegevensbescherming van De Vitalis Zorg Groep (FG)
- ( ) Aangemeld bij het College Bescherming Persoonsgegevens in Den Haag (CBP)

Werking
Om een volledig beeld te krijgen van de beschreven verwerking is enig inzicht in de werking ervan noodzakelijk. Een beschrijving van hoe de verwerking werkt is geen formele wettelijke eis, maar een toevoeging in dit onderzoek om ook onderlinge vergelijking van de verwerkingen mogelijk te maken.

Vraag 1.12

Geef a.u.b een korte omschrijving van hoe deze verwerking werkt?

Terugkoppeling van ingevulde gegevens

Als u via e-mail een kopie wilt ontvangen van de ingevulde gegevens, vult u dan hieronder uw volledige e-mail-adres in (dus in de vorm voorletter.tussenvoegsel.achternaam@vitalis-zorggroep.nl, bijvoorbeeld s.vander.pol@vitalis-zorggroep.nl).

Antwoorden wissen en opnieuw beginnen | Formulier versturen | 05.04.02

Bijlage 3: uitgewerkt interviewschema t.b.v. quick-scan

Toelichting op de WBP Quick Scan
De Vitalis Zorg Groep is, zoals alle organisaties die persoonlijke gegevens beheren en/of verwerken, verplicht zich te houden aan de Wet Bescherming Persoonsgegevens (WBP) en andere privacyregels. Deze wet geeft aan wat de rechten zijn van iemand van wie gegevens worden gebruikt en wat de verplichtingen zijn van organisaties die gegevens gebruiken. Verzamelen en verwerken van persoonsgegevens dient te geschieden onder de voorwaarden en verplichtingen, zoals gesteld in de WBP.

De eisen die de WBP stelt zijn te verdelen in 6 hoofdcategorieën, te weten:

- transparantie,
- doelbinding,
- rechtmatige grondslag,
- kwaliteit van de gegevens,
- beveiliging,
- bewaartermijnen.

Binnen deze quick-scan, die onderdeel is van een organisatiebreed onderzoek naar de WBP binnen De Vitalis Zorg Groep, wordt onderzocht in hoeverre de organisatie voldoet aan de eisen die de WBP stelt. Daarnaast wordt ook onderzocht wat de ambities zijn van de organisatie op de verschillende deelgebieden van de WBP. Dit alles gebeurt op een vrij hoog abstractieniveau. Pas in het derde deel van het onderzoek zal, bij een beperkte groep deelnemers, op detailniveau worden onderzocht wat de status van de WBP binnen Vitalis precies is.

Voor elke categorie uit de WBP zijn in dit deel van het onderzoek telkens twee multiple-choice vragen gedefinieerd: één gericht op de huidige situatie en één gericht op de ambitie. Per vraag worden de gebruikte begrippen toegelicht en wordt een korte invulinstructie gegeven.
De vragen moeten worden beantwoord vanuit uw eigen plaats in de organisatie en vanuit de verwerkingen waar u toegang tot heeft of waar u gebruik van maakt. Een oordeel geven over verwerkingen die buiten uw gezichtsveld liggen of over organisatieonderdelen buiten die van u zelf is dus niet nodig.

De gegevens die u verstrekt zullen anoniem worden verwerkt, dat wil zeggen dat alleen de onderzoekers inzage hebben in uw persoonlijke gegevens. De resultaten zullen anoniem worden gepresenteerd aan de Raad van Bestuur en samenvattingen worden verstuurd naar de directies en hoofden ondersteunende diensten.

Mocht u nog vragen hebben, neem dan gerust contact op met S. van der Pol (**s.vander.pol@vitalis-zorggroep.nl**), telefoon: 040-2933526

Alvast dank voor uw medewerking,

Introductie begrippen uit de Wet Bescherming Persoonsgegevens

Persoonsgegevens.

Gegevens zijn persoonsgegevens als deze gegevens informatie bevatten over een natuurlijke persoon en die persoon identificeerbaar is. Identificeerbaar is deze persoon uiteraard als er een naam wordt opgeslagen, maar ook andere gegevens die het mogelijk maken achter deze naam te komen vallen het begrip "persoonsgegevens". Voorbeelden hiervan zijn een telefoonnummer, het kenteken van een auto, een kamernummer, sofi-nummer, kortom alle gegevens waarmee je achter de identiteit van de persoon over wie het gaat kunt komen. De WBP noemt de persoon van wie persoonsgegevens verwerkt worden "de betrokkene".

In de praktijk kunnen dit gegevens zijn van zowel bewoners, medewerkers, vrijwilligers, externe hulpverleners of combinaties hiervan in de vorm van adreslijstjes, maaltijdregistraties, adresgegevens van bewoners of relaties van bewoners, de e-mailadressen zoals die op het netwerk staan, een overzicht van de welzijnsmeldingen enz. enz.

Verwerkingen.

Een gegevensverwerking is het hele proces dat een persoonsgegeven doormaakt, vanaf het moment dat het wordt verkregen tot en met het moment dat het wordt vernietigd (een samenhangend geheel van handelingen binnen één totaal computerprogramma bijvoorbeeld de salarisadministratie of de bewonersadministratie).

Daarnaast valt ook elke afzonderlijke technische- of verwerkingshandeling onder het begrip "verwerking" (verwerking in de

enkelvoudige betekenis zoals opslaan, kopiëren, mailen of printen).

Voor deze inventarisatie betekent dit dat alle (computer)bestanden en programma's die binnen Vitalis in gebruik zijn onder het begrip verwerking vallen en dat deze meegenomen moeten worden in de beoordeling, behalve de uitzonderingen die hieronder worden beschreven.

Uitzonderingen die niet beschreven hoeven te worden.

De wet is niet van toepassing op verwerkingen voor persoonlijk of huishoudelijk gebruik. Onder deze uitzondering vallen o.a. persoonlijke aantekeningen of adresbestanden die slechts door één persoon en voor zichzelf worden gebruikt. Deze behoeven dus niet te worden meegenomen in deze inventarisatie.

Uw naam:

Naam van uw lokatie of dienst:

Transparantie

Het gaat bij het transparantiebeginsel om het recht van betrokkenen om kennis te nemen van en geïnformeerd te worden over het feit dat er een geautomatiseerde verwerking met zijn/haar gegevens bestaat, de doeleinden van deze verwerking en de identiteit van de verantwoordelijke. Om dit te kunnen vaststellen is het van belang dat betrokkenen weten waar, wanneer en door wie persoonsgegevens worden verwerkt.

Ook het recht van toegang tot deze verwerking maakt onderdeel uit van het transparantiebeginsel. Betrokkenen hebben het recht om vrijelijk, zonder beperking en zonder bovenmatige vertraging of kosten geïnformeerd te worden over het bestaan van verwerkingen, de doeleinden van deze verwerking, de (categorieën van) gegevens die verwerkt worden en de ontvangers aan wie deze gegevens worden verstrekt.

Vraag 2.1.0a
Hoe beoordeelt u de huidige manier waarop de organisatie omgaat met de transparantie van gegevenverwerkingen en het informeren van de betrokkenen? Onder procedures worden de formele MIK-V documenten verstaan.
Kies een van deze alternatieven:

- (●) Er zijn **geen** vastgelegde procedures en de verplichting tot informeren is **niet** in de organisatie bekend
- ( ) Er zijn **geen** vastgelegde procedures maar de verplichting tot informeren is **wel** in de organisatie bekend
- ( ) Er zijn **geen** vastgelegde procedures maar de betrokkenen worden **wel** consequent geïnformeerd
- ( ) Er zijn **wel** procedures vastgelegd **en** deze worden nageleefd
- ( ) Er zijn **wel** procedures vastgelegd welke **wel** worden nageleefd **en** waarvan de naleving periodiek wordt gecontroleerd

Vraag 2.1.0.b
Wat is volgens u het streefniveau waarop de organisatie dient te komen voor wat betreft de transparantie van verwerkingen en het informeren van betrokkenen?
Kies een van deze alternatieven:

- Er zijn **geen** vastgelegde procedures maar de betrokkenen worden **wel** consequent geïnformeerd
- Er zijn **wel** procedures vastgelegd **en** deze worden nageleefd
- Er zijn **wel** procedures vastgelegd welke **wel** worden nageleefd **en** waarvan de naleving periodiek wordt gecontroleerd

---

Doelbinding
Doelbinding betekent dat gegevens alleen maar mogen worden verwerkt onder welbepaalde, vooraf uitdrukkelijk omschreven en gerechtvaardigde doeleinden. De verzamelde gegevens mogen daarnaast niet worden gebruikt voor doeleinden die niet met het oorspronkelijke doel verenigbaar zijn. Dit betekent in de praktijk dat voor elke verwerking vooraf duidelijk moet zijn omschreven wat het doel is en dat de verwerkte gegevens niet voor een ander, onverenigbaar, doel mogen worden gebruikt.

Vraag 2.2.0a
Hoe beoordeelt u de huidige manier waarop de organisatie omgaat met het beginsel van doelbinding van gegevenverwerkingen, het vooraf omschrijven van het doel van de verwerking en verwerken van gegevens voor verenigbare doelen? Onder procedures worden de formele MIK-V documenten verstaan.
Kies een van deze alternatieven:

- (●) Er zijn **geen** vastgelegde procedures voor het verzamelen en verder verwerken en de regels voortvloeiend uit doelbinding zijn **niet** in de organisatie bekend
- Er zijn **geen** vastgelegde procedures maar de regels voortvloeiend uit doelbinding voor verzamelen en verder verwerken zijn **wel** in de organisatie bekend
- Er zijn **geen** vastgelegde procedures maar de regels en verplichtingen volgende uit doelbinding worden **wel** consequent nageleefd
- Er zijn **wel** procedures vastgelegd **en** deze worden nageleefd
- Er zijn **wel** procedures vastgelegd welke **wel** worden nageleefd **en** waarvan de naleving periodiek wordt gecontroleerd

Vraag 2.2.0b
Wat is volgens u het streefniveau waarop de organisatie dient te komen voor wat betreft de doelbinding van gegevenverwerkingen, het vooraf omschrijven van het doel van de verwerking en verwerken van gegevens voor verenigbare doelen?
Kies een van deze alternatieven:

- (●) Er zijn **geen** vastgelegde procedures voor het verzamelen en verder verwerken en de regels voortvloeiend uit doelbinding zijn **niet** in de organisatie bekend
- Er zijn **geen** vastgelegde procedures maar de regels voortvloeiend uit doelbinding voor verzamelen en verder verwerken zijn **wel** in de organisatie bekend
- Er zijn **geen** vastgelegde procedures maar de regels en verplichtingen volgende uit doelbinding worden **wel** consequent nageleefd
- Er zijn **wel** procedures vastgelegd **en** deze worden nageleefd
- Er zijn **wel** procedures vastgelegd welke **wel** worden nageleefd **en** waarvan de naleving periodiek wordt gecontroleerd

De wet stelt de eis dat er een rechtmatige grondslag moet zijn voor de verwerking; persoonsgegevens mogen alleen worden verzameld en verwerkt wanneer de grondslag hiervoor in de WBP kan worden gevonden. De WBP geeft een zestal grondslagen voor verwerking waarvan er minimaal één van toepassing moet zijn; elke gegevensverwerking of categorie van verwerkingen dient herleidbaar te zijn tot een van de, limitatief in de wet, benoemde grondslagen. Voor bijzondere persoonsgegevens zoals godsdienst, ras, gezondheid, politieke gezindheid of seksuele leven gelden zelfs nog aanvullende, specifieke regels, gebaseerd op het uitgangspunt dat bijzondere persoonsgegevens niet mogen worden verwerkt tenzij daarvoor een wettelijke mogelijkheid is gegeven.

Vraag 2.3.0a
Hoe beoordeelt u de huidige manier waarop de organisatie omgaat met het beginsel van rechtmatige grondslag van gegevenverwerkingen en de aansluiting met de grondslagen zoals deze in de wet worden gegeven? Onder procedures worden de formele MIK-V documenten verstaan.
Kies een van deze alternatieven:

- (●) Er zijn **geen** vastgelegde procedures voor het bepalen van de rechtmatige grondslag van verwerking en de regels c.q. verplichtingen voortvloeiend uit de eis van rechtmatigheid zijn **niet** in de organisatie bekend
- ( ) Er zijn **geen** vastgelegde procedures maar de regels en verplichtingen voortvloeiend uit de eis van rechtmatigheid zijn **wel** in de organisatie bekend
- ( ) Er zijn **geen** vastgelegde procedures maar de regels voor rechtmatigheid van de verwerkingen op basis van de wet wordt **wel** consequent nageleefd
- ( ) Er zijn **wel** procedures vastgelegd **en** deze worden nageleefd
- ( ) Er zijn **wel** procedures vastgelegd welke **wel** worden nageleefd **en** waarvan de naleving periodiek wordt gecontroleerd

Vraag 2.3.0b
Wat is volgens u het streefniveau waarop de organisatie dient te komen voor wat betreft het beginsel van rechtmatige grondslag van gegevenverwerkingen en de aansluiting met de grondslagen zoals deze in de wet worden gegeven?
Kies een van deze alternatieven:

- (●) Er zijn **geen** vastgelegde procedures voor het bepalen van de rechtmatige grondslag van verwerking en de regels c.q. verplichtingen voortvloeiend uit de eis van rechtmatigheid zijn **niet** in de organisatie bekend
- ( ) Er zijn **geen** vastgelegde procedures maar de regels en verplichtingen voortvloeiend uit de eis van rechtmatigheid zijn **wel** in de organisatie bekend
- ( ) Er zijn **geen** vastgelegde procedures maar de regels voor rechtmatigheid van de verwerkingen op basis van de wet wordt **wel** consequent nageleefd
- ( ) Er zijn **wel** procedures vastgelegd **en** deze worden nageleefd
- ( ) Er zijn **wel** procedures vastgelegd welke **wel** worden nageleefd **en** waarvan de naleving periodiek wordt gecontroleerd

---

Kwaliteit van gegevens
Het kwaliteitsbeginsel valt in twee onderdelen uiteen: de verzamelde persoonsgegevens moeten relevant zijn voor het doel waarvoor zij worden verwerkt ofwel de gegevens moeten toereikend, ter zake dienend en niet overmatig zijn in relatie tot het doel waarvoor ze worden verwerkt. Daarnaast moeten de persoonsgegevens juist, accuraat, volledig en actueel zijn. Dit impliceert mede dat ze, indien nodig, worden bijgewerkt en dat er redelijke maatregelen zijn getroffen om onjuistheden, fouten en tekortkomingen te herstellen.

Vraag 2.4.0a
Hoe beoordeelt u de huidige manier waarop de organisatie omgaat met het kwaliteitsbeginsel en de aansluiting met de eisen aan verwerkingen zoals hierboven genoemd? Onder procedures worden de formele MIK-V documenten verstaan.
Kies een van deze alternatieven:

- (●) Er zijn **geen** vastgelegde procedures en de regels c.q. kwaliteitseisen zijn **niet** in de organisatie bekend
- ( ) Er zijn **geen** vastgelegde procedures maar de regels c.q. kwaliteitseisen zijn **wel** in de organisatie bekend
- ( ) Er zijn **geen** vastgelegde procedures maar de regels c.q. kwaliteitseisen worden **wel** consequent nageleefd
- ( ) Er zijn **wel** procedures vastgelegd **en** deze worden nageleefd
- ( ) Er zijn **wel** procedures vastgelegd welke **wel** worden nageleefd **en** waarvan de naleving periodiek wordt gecontroleerd

Vraag 2.4.0b
Wat is volgens u het streefniveau waarop de organisatie dient te komen voor wat betreft het kwaliteitsbeginsel en de aansluiting met de eisen aan verwerkingen zoals hierboven genoemd?
Kies een van deze alternatieven:

- (●) Er zijn **geen** vastgelegde procedures en de regels c.q. kwaliteitseisen zijn **niet** in de organisatie bekend
- ( ) Er zijn **geen** vastgelegde procedures maar de regels c.q. kwaliteitseisen zijn **wel** in de organisatie bekend
- ( ) Er zijn **geen** vastgelegde procedures maar de regels c.q. kwaliteitseisen worden **wel** consequent nageleefd
- ( ) Er zijn **wel** procedures vastgelegd **en** deze worden nageleefd
- ( ) Er zijn **wel** procedures vastgelegd welke **wel** worden nageleefd **en** waarvan de naleving periodiek wordt gecontroleerd

---

Beveiliging
De essentie hier is dat de verantwoordelijke ervoor zorg draagt dat alle passende technische en organisatorische maatregelen worden getroffen om verlies, beschadiging of onrechtmatige verwerking van gegevens te voorkomen. Ook moeten er zo min mogelijk gegevens worden gebruikt die herleidbaar zijn tot individuele personen. De maatregelen ter beveiliging kunnen in drie soorten worden onderscheiden:

- Geheimhoudingsplicht; degenen die persoonsgegevens verwerken moeten hiertoe, van de verantwoordelijke, de bevoegdheid hebben gekregen. Ook hebben deze medewerkers een geheimhoudingsplicht over de gegevens waar zij toegang tot hebben.
- Passende technische en organisatorische maatregelen tegen verlies en onrechtmatige verwerking.
- De deugdelijkheid van de beveiligingsmaatregelen die een bewerker (een derde partij) neemt bij het verwerken van persoonsgegevens in opdracht van De Vitalis Zorg Groep.

Vraag 2.5.0a
Hoe beoordeelt u de huidige manier waarop de organisatie omgaat met de beveiliging van persoonsgegevens en de aandacht voor de hierboven genoemde maatregelen? Onder procedures worden de formele MIK-V documenten verstaan.
Kies een van deze alternatieven:

- (●) Er zijn **geen** vastgelegde procedures voor gegevensbeveiliging en de regels c.q. beveiligingsmaatregelen zijn **niet** in de organisatie bekend
- ( ) Er zijn **geen** vastgelegde procedures voor gegevensbeveiliging maar de regels c.q. beveiligingsmaatregelen zijn **wel** in de organisatie bekend

Er zijn **wel** procedures vastgelegd **en** deze worden nageleefd

Er zijn **wel** procedures vastgelegd welke **wel** worden nageleefd **en** waarvan de naleving periodiek wordt gecontroleerd

Vraag 2.5.0b
Wat is volgens u het streefniveau waarop de organisatie dient te komen voor wat betreft omgang met de beveiliging van persoonsgegevens en de aandacht voor de hierboven genoemde maatregelen?
Kies een van deze alternatieven:

Er zijn **geen** vastgelegde procedures voor gegevensbeveiliging en de regels c.q. beveiligingsmaatregelen zijn **niet** in de organisatie bekend

Er zijn **geen** vastgelegde procedures voor gegevensbeveiliging maar de regels c.q. beveiligingsmaatregelen zijn **wel** in de organisatie bekend

Er zijn **geen** vastgelegde procedures maar de regels c.q. beveiligingsmaatregelen worden **wel** consequent nageleefd

Er zijn **wel** procedures vastgelegd **en** deze worden nageleefd

Er zijn **wel** procedures vastgelegd welke **wel** worden nageleefd **en** waarvan de naleving periodiek wordt gecontroleerd

---

Bewaartermijnen
Persoonsgegevens mogen niet langer worden bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren dan noodzakelijk is voor het bereiken van het doel waarvoor deze zijn verzameld. Men dient zich dan ook telkens af te vragen of er nog voldoende redenen zijn waarom de gegevens bewaard dienen te blijven. Zijn deze redenen aanwezig dan kan de verantwoordelijke bepalen welke bewaartermijnen op deze gegevens van toepassing zijn. Zijn deze redenen er niet, dan mogen de gegevens niet meer verwerkt worden tenzij voor een ander, verenigbaar doel. Voor verwerkingen die aan bepaalde voorwaarden voldoen zijn in het vrijstellingsbesluit duidelijke bewaartermijnen gegeven. Voor bepaalde categorieën van persoonsgegevens gelden specifieke bewaartermijnen uit andere wetten die voorgaan op de bepaling uit de WBP

Vraag 2.6.0a
Hoe beoordeelt u de huidige manier waarop de organisatie omgaat met het bewaren van persoonsgegevens en de hiervoor geldende termijnen? Onder procedures worden de formele MIK-V documenten verstaan.
Kies een van deze alternatieven:

Er zijn **geen** vastgelegde procedures voor het bewaren van persoonsgegevens en de toepasselijke bewaartermijnen zijn **niet** in de organisatie bekend

Er zijn **geen** vastgelegde procedures voor het bewaren van persoonsgegevens maar de toepasselijke termijnen zijn **wel** in de organisatie bekend

Er zijn **geen** vastgelegde procedures maar de toepasselijke bewaartermijnen worden **wel** consequent nageleefd

Er zijn **wel** procedures vastgelegd **en** deze worden nageleefd

Er zijn **wel** procedures vastgelegd welke **wel** worden nageleefd **en** waarvan de naleving periodiek wordt gecontroleerd

Vraag 2.6.0b
Wat is volgens u het streefniveau waarop de organisatie dient te komen voor wat betreft het bewaren van persoonsgegevens en de hiervoor geldende termijnen?
Kies een van deze alternatieven:

- (•) Er zijn **geen** vastgelegde procedures voor het bewaren van persoonsgegevens en de toepasselijke bewaartermijnen zijn **niet** in de organisatie bekend
- ( ) Er zijn **geen** vastgelegde procedures voor het bewaren van persoonsgegevens maar de toepasselijke termijnen zijn **wel** in de organisatie bekend
- ( ) Er zijn **geen** vastgelegde procedures maar de toepasselijke bewaartermijnen worden **wel** consequent nageleefd
- ( ) Er zijn **wel** procedures vastgelegd **en** deze worden nageleefd
- ( ) Er zijn **wel** procedures vastgelegd welke **wel** worden nageleefd **en** waarvan de naleving periodiek wordt gecontroleerd

★

Afsluiting

Heeft u nog op- of aanmerkingen op deze enquête of op de consequenties van de WBP in het algemeen, vul ze dan s.v.p. hieronder in.

Terugkoppeling van ingevulde gegevens

Als u via e-mail een kopie wilt ontvangen van de ingevulde gegevens, vult u dan hieronder uw volledige e-mail-adres in (dus in de vorm voorletter.tussenvoegsel.achternaam@vitalis-zorggroep.nl, bijvoorbeeld s.vander.pol@vitalis-zorggroep.nl)

Antwoorden wissen | Formulier versturen | 05.04.05

Bijlage 4: uitgewerkt interviewschema t.b.v. diepte-interviews.

Transparantie

Nr.	Sub	Interviewvraag	Antwoordsysteem
2.1.1		Zijn de gegevens die in de verwerkingen zijn opgenomen rechtstreeks van de betrokkene verkregen?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.1.2		Kan informatieverstrekking over de kenmerken van de verwerkingen aan betrokkenen achterwege blijven? Informatieverstrekking kan achterwege blijven in één van de volgende gevallen: o De betrokkenen was al op de hoogte van het feit dat deze gegevens zijn opgenomen in een verwerking, o Het kost onevenredige inspanning om de betrokkenen te informeren over de verwerking, o De verwerking is voorgeschreven door de wet.	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.1.3		Worden betrokkenen direct geïnformeerd over de verwerking van zijn gegevens?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.1.4		Worden betrokkenen geïnformeerd over doel van de verwerking en identiteit van de verantwoordelijke?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.1.5		Is het voor betrokkenen duidelijk waar, hoe en bij wie een verzoek tot inzage in zijn gegevens moet worden ingediend?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.1.6		Zijn er termijnen afgesproken waarbinnen een reactie op een verzoek van betrokkenen moet worden gegeven?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.1.7		Als gereageerd wordt op een verzoek tot inzage, welke gegevens bevat deze respons dan?	Open vraag, Omschrijf de inhoud van een reactie op een verzoek tot inzage.....
2.1.8		Hoe kan een derde, niet zijnde de betrokkene, reageren op een voorgenomen informatieverstrekking naar betrokkene?	Open vraag, Omschrijf de wijze waarop een derde zijn reactie kenbaar kan maken.....
2.1.9	a	Hoe wordt er omgegaan met een verzoek tot inzage dat niet schriftelijk wordt ingediend door betrokkene?	Open vraag, Omschrijf de wijze waarop met een niet-schriftelijk verzoek wordt omgegaan.....
	b	Hoe wordt er omgegaan met een verzoek tot inzage dat niet door maar namens betrokkene wordt ingediend?	Open vraag, Omschrijf de wijze waarop met een verzoek namens betrokkene wordt omgegaan.....
2.1.10		Wordt de identiteit van een verzoeker geverifieerd?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.1.11		Is het voor betrokkenen duidelijk waar, hoe en bij wie een verzoek tot wijziging van zijn gegevens moet worden ingediend?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd

			○ Weet niet
2.1.12		Op welke manieren wordt gereageerd op een verzoek tot wijziging?	Gesloten vraag; kies een of meerdere van deze alternatieven: ○ Wijziging uitgevoerd, ○ Wijzigingsverzoek afgewezen, ○ Wijziging onmogelijk ○ Anders, namelijk.....
2.1.13		Worden aangebrachte wijzigingen doorgegeven aan derden?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.1.14		Is het voor betrokkenen duidelijk waar, hoe en bij wie verzet moet worden ingediend?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.1.15		Is betrokkene gewezen op de mogelijk van absoluut verzet?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.1.16		Indien er sprake is van absoluut verzet dan wel gerechtvaardigd relatief verzet, zijn er maatregelen getroffen om de verwerking terstond te beëindigen?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.1.17		Worden er besluiten genomen die uitsluitend zijn gebaseerd op geautomatiseerde verwerking?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.1.18		Is er voor de gevallen waarin een geautomatiseerd besluit wordt genomen een wettelijke grondslag?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet

Doelbinding

Nr.	Sub	Interviewvraag	Antwoordsysteem
2.2.1		Is er een verschil tussen het doel waarvoor de gegevens zijn verkregen en het doel waarvoor ze worden verwerkt? Hierbij kan gebruik gemaakt worden van de benoemde “zorgproducten” en de differentiatie in “personeelsdiensten” uit paragraaf 5.3 en de concretisering hiervan in het Vrijstellingsbesluit	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.2.2		Als er meerdere gegevens worden verwerkt, vallen de verwerkte gegevens in dezelfde categorie? Hier kan de beschrijving uit paragraaf 5.2.6 ondersteunend zijn in combinatie met de opsommingen van gegevens die worden gebruikt in het Vrijstellingsbesluit.	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet

Rechtmatige grondslag

Nr.	Sub	Interviewvraag	Antwoordsysteem
2.3.1		Wordt gecontroleerd of betrokkene toestemming heeft gegeven voor de verwerking?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.3.2		Wordt het onderscheid tussen ondubbelzinnige en uitdrukkelijke toestemming gecontroleerd?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen)

			○ Altijd ○ Weet niet
2.3.3		Wordt gecontroleerd of er sprake is van een (pre) contractuele verplichting tussen verantwoordelijke en betrokkene?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.3.4		Wordt gecontroleerd of de verwerking noodzakelijk is voor nakoming van de (pre) contractuele verplichting?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd Weet niet
2.3.5		Wordt gecontroleerd of er een wettelijke verplichting is voor verwerking?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.3.6		Is het zonder de verwerking redelijkerwijs onmogelijk om aan de wettelijke verplichting te voldoen?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.3.7		Indien geen toestemming van betrokkene gevraagd is, is er dan een voldoende levensbedreigende omstandigheid die het vragen van toestemming uitsluit?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.3.8		Is er sprake van een voldoende (medische) noodzaak tot verwerking?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.3.9		Als verwerking van de gegevens noodzakelijk is voor het functioneren van de organisatie, zijn er dan maatregelen genomen die ervoor zorgen dat de belangen van de betrokkene worden afgewogen en er geen inbreuk wordt gemaakt op de rechten van betrokkene?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.3.10		Wordt er bij verwerking gecontroleerd of het beoogde doel ook langs andere weg kan worden gerealiseerd?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet

Kwaliteit

Nr.	Sub	Interviewvraag	Antwoordsysteem
2.4.1		Worden de gegevens bij de bron gevalideerd, gecontroleerd en verwerkt?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.4.2		Is er een controle op de relatie tussen verwerkte gegevens en het beoogde doel van de verwerking?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.4.3		Worden gegevens bij uitvoer en gebruik gecontroleerd op juistheid en actualiteit?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.4.4		Zijn er maatregelen genomen om het moment van	Gesloten vraag; kies een van deze alternatieven:

		ontstaan van onjuistheden te achterhalen?	○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.4.5		Zijn er maatregelen genomen om geconstateerde onjuistheden te verbeteren?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet

Beveiliging

Beveiligingsbeleid

Nr.	Sub	Interviewvraag	Antwoordsysteem
2.5.1		Is binnen uw organisatie afgesproken (en vastgelegd) hoe met informatiebeveiliging wordt omgegaan (wat wordt eraan gedaan en wat willen we eraan doen)?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.5.2		Is afgesproken wie er eindverantwoordelijk is voor het onderwerp binnen uw organisatie?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.5.3		Wordt regelmatig bekeken wat er van de plannen op het gebied van informatiebeveiliging binnen uw organisatie is terechtgekomen?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.5.4		Is er een beleidsdocument voor informatiebeveiliging opgesteld met als scope de organisatie en de aangeslotenen?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.5.5		Vindt periodiek een beoordeling en evaluatie plaats van het totale informatiebeveiligingsbeleid?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet

Organiseren van informatiebeveiliging

Nr.	Sub	Interviewvraag	Antwoordsysteem
2.6.1		Is binnen de organisatie besproken wie verantwoordelijk is voor het in gebruik nemen van nieuwe IT-middelen (of andere informatiemiddelen).	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.6.2		Zijn er met 'derden' (zoals onderhoudspersonen hard- en software, schoonmaakpersoneel, tijdelijke krachten) afspraken gemaakt over toegang tot ruimten en informatiemiddelen?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.6.3		Als ICT-activiteiten zijn uitbesteedt, is er dan in contracten duidelijkheid over informatiebeveiliging?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.6.4		Wordt er aandacht besteedt aan opleiding van medewerkers voor wat betreft informatiebeveiliging?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen)

			○ Altijd Weet niet
2.6.5		Beschikt de organisatie over een beveiligingsadviseur of een contactpersoon voor informatiebeveiliging?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.6.6		Heeft de beveiligingsadviseur of de contactpersoon voor informatiebeveiliging contacten met andere beveiligingsadviseurs uit bedrijfsleven of overheid?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.6.7		Is een multidisciplinair forum aanwezig, bestaande uit managers of afgevaardigden van alle aangeslotenen en de ICT-organisatie zelf, die de implementatie van maatregelen voor informatiebeveiliging coördineert?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.6.8		Zijn de verantwoordelijkheden voor de bescherming van individuele bedrijfsmiddelen en voor het uitvoeren van bepaalde beveiligingsprocessen duidelijk gedefinieerd?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.6.9		Wordt de implementatie van de informatiebeveiliging regelmatig beoordeeld door een onafhankelijke instantie?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.6.10		Worden de risico's geanalyseerd die ontstaan doordat externe gebruikers (aangeslotenen) fysieke en/of logische toegang hebben tot informatieverwerkende voorzieningen?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.6.11		Zijn beveiligingseisen gespecificeerd in contracten met derden die betrekking hebben op de toegang tot de informatieverwerkende voorzieningen van de organisatie?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.6.12		Worden beveiligingseisen opgenomen in de uitbestedingscontracten met derden?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet

Beheer van middelen voor informatievoorziening

Nr.	Sub	Interviewvraag	Antwoordsysteem
2.7.1		Is voor alle informatievoorzieningmiddelen (computers, faxen, netwerkinfrastructuur, etc.) afgesproken wie er verantwoordelijk is voor onderhoud, integriteit enzovoorts?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.7.2		Wordt bij het beveiligen van informatie onderscheid gemaakt voor wat betreft het soort informatie waar het over gaat (b.v. heel vertrouwelijk versus voor iedereen toegankelijk)?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.7.3		Maakt de men gebruik van beveiligingsclassificaties voor kritische en gevoelige informatie, teneinde het vereiste beveiligingsniveau te kunnen aangeven?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.7.4		Zijn er over het omgaan met die soorten informatie afspraken vastgelegd?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit

			○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet

Beveiligingseisen ten aanzien van personeel

Nr.	Sub	Interviewvraag	Antwoordsysteem
2.8.1		Zijn beveiligingstaken en -verantwoordelijkheden, zoals vastgelegd in het beveiligingsbeleid, opgenomen in functieomschrijvingen?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.8.2		Worden sollicitanten naar een functie waarbij men toegang heeft tot gevoelige informatie, gescreend alvorens zij worden aangenomen?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.8.3		Moeten medewerkers een geheimhoudingsverklaring ondertekenen?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.8.4		Is in het arbeidscontract opgenomen dat de medewerker een verantwoordelijkheid heeft op het gebied van informatiebeveiliging?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.8.5		Wordt er binnen de organisatie aandacht besteedt aan het overbrengen van het hoe en wat met betrekking tot informatiebeveiliging op de medewerkers?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.8.6		Worden alle aangeslotenen op passende wijze getraind in beveiligingsprocedures en de bijbehorende technieken?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.8.7		Zijn binnen de organisatie afspraken gemaakt over hoe om te gaan met beveiligingsincidenten?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.8.8		Worden incidenten op de een of andere manier vastgelegd?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.8.9		Zijn procedures vastgesteld voor het melden door de aangeslotenen en afhandelen van beveiligingsincidenten?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.8.10		Zijn de aangeslotenen verplicht om alle zwakke plekken, die zij opmerken of vermoeden in de beveiliging van systemen of diensten van de ICT-organisatie, te noteren en te rapporteren?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.8.11		Is een mechanisme aanwezig die de netwerkorganisatie in staat stelt de aard, de omvang en de kosten van incidenten en storingen te kwantificeren en te bewaken?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet

2.8.12		Worden inbreuken op de beveiliging door middel van een formeel disciplinair proces afgehandeld?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet

Fysieke beveiliging en beveiliging van de omgeving

Nr.	Sub	Interviewvraag	Antwoordsysteem
2.9.1		Maakt de organisatie onderscheid naar verschillende beveiligingsniveaus om gebieden die IT-voorzieningen bevatten te beschermen?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.9.2		Worden beveiligde zones beschermd door een adequate toegangsbeveiliging, zodat alleen geautoriseerd personeel toegang heeft?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.9.3		Wordt bij de keuze en het ontwerp van een beveiligde zone rekening gehouden met de mogelijkheid van schade door fysieke bedreigingen, zoals brand, wateroverlast, explosie en dergelijke?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.9.4		Zijn additionele richtlijnen en maatregelen aanwezig om de beveiliging van beveiligde ruimten te kunnen waarborgen?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.9.5		Wordt apparatuur zodanig geplaatst en beveiligd dat de risico's van schade, storing en ongeautoriseerd gebruik minimaal zijn?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.9.6		Is apparatuur beveiligd tegen stroomstoringen en andere elektrische storingen?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.9.7		Is de bekabeling voor dataverkeer en voor ondersteunende informatiediensten beschermd tegen interceptie of beschadiging?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.9.8		Wordt alle apparatuur op correcte wijze onderhouden?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.9.9		Gelden beveiligingsprocedures en beveiligingsmaatregelen ook voor apparatuur die, door de medewerker buiten de organisatie wordt gebruikt?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.9.10		Wordt apparatuur gecontroleerd op de aanwezigheid van opgeslagen gegevens en in licentie gebruikte software, voordat de apparatuur wordt afgevoerd?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.9.11		Is een clear desk en clear screen policy ingevoerd?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen)

			○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.9.12		Zijn maatregelen getroffen om te voorkomen dat het personeel zonder toestemming eigendommen van de organisatie meeneemt?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet

Operationeel beheer van voorzieningen

Nr.	Sub	Interviewvraag	Antwoordsysteem
2.10.1		Zijn schriftelijke procedures opgesteld voor de bediening van alle IT-voorzieningen?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.10.2		Zijn formele procedures aanwezig met betrekking tot de controle op wijzigingen in IT-voorzieningen en informatiesystemen?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.10.3		Is bepaald wie wat mag met betrekking tot het toevoegen, wijzigen en verwijderen van informatie?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.10.4		Zijn verantwoordelijkheden en procedures vastgesteld voor de afhandeling van beveiligingsincidenten?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.10.5		Wordt functiescheiding toegepast om de kans op ongeautoriseerde wijzigingen of opzettelijk misbruik van informatie of diensten te verkleinen?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.10.6		Zijn de voorzieningen voor het ontwikkelen en testen van systemen gescheiden van operationele systemen?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.10.7		Zijn, in het geval van uitbesteding van het beheer van IT-voorzieningen, passende beveiligingsmaatregelen met de contractant overeengekomen en zijn deze opgenomen in het contract?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.10.8		Worden de capaciteitseisen gemonitored en wordt een prognose gemaakt van toekomstige eisen, teneinde storingen ten gevolge van een gebrek aan capaciteit te voorkomen?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.10.9		Worden acceptatiecriteria gedefinieerd, besproken, gedocumenteerd en getest alvorens nieuwe informatiesystemen te accepteren?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.10.10		Zijn maatregelen ingevoerd voor de preventie en detectie van kwaadaardige software, zoals virussen?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.10.11		Worden regelmatig reservekopieën gemaakt van	Gesloten vraag; kies een van deze alternatieven:

		essentiële zakelijke informatie en software?	○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.10.12		Houden de systeembeheerders een logboek bij van de werkzaamheden die zij verrichten?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.10.13		Worden, door de aangeslotenen gemelde, storingen vastgelegd in een logboek?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.10.14		Zijn adequate maatregelen getroffen voor de beveiliging van gegevens in netwerken en de bescherming van de aangeslotenen tegen ongeautoriseerde toegang?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.10.15		Zijn procedures opgesteld voor het beheer van verwijderbare computermedia zoals banden, schijven, cassettes en afgedrukte rapporten?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.10.16		Worden media op een veilige manier afgevoerd wanneer zij niet langer nodig zijn?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.10.17		Zijn procedures opgesteld voor de behandeling en opslag van informatie ter bescherming tegen ongeoorloofde openbaarmaking of misbruik?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.10.18		Is systeemdocumentatie beveiligd tegen ongeautoriseerde toegang?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.10.19		Zijn in overeenkomsten met de aangeslotenen en 'derden' beveiligingsmaatregelen met betrekking tot het uitwisselen van informatie en software opgenomen?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.10.20		Zijn maatregelen genomen ter beveiliging van computermedia tijdens vervoer tegen misbruik of verlies?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.10.21		Zijn speciale maatregelen getroffen ter beveiliging van elektronische handel die nodig kunnen zijn om o.a. frauduleuze handelingen, contractgeschillen en ongewilde openbaring of manipulatie van informatie te voorkomen?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.10.22		Zijn speciale maatregelen getroffen voor de beperking van de risico's van het gebruik van elektronische post?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.10.23		Zijn duidelijke richtlijnen en procedures opgesteld voor de beheersing van de risico's die elektronische	Gesloten vraag; kies een van deze alternatieven: ○ Nooit

		kantoorsystemen met zich meebrengen?	○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.10.24		Is aandacht besteed aan de bescherming van de integriteit van elektronisch gepubliceerde informatie, om te voorkomen dat de reputatie van de uitgevende organisatie beschadigd raakt doordat ongeautoriseerde wijzigingen plaatsvinden?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet

Toegangsbeveiliging

Nr.	Sub	Interviewvraag	Antwoordsysteem
2.11.1		Wordt er gebruik gemaakt van 'autorisatieprofielen' (welke medewerker mag wat) met betrekking tot toegang tot informatie en ICT-middelen?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.11.2		Is er een noodprocedure die toegang in noodgevallen regelt?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.11.3		Is een beleid vastgesteld ten aanzien van toegangsbeveiliging waarin de eisen en de regels voor toegangsbeveiliging zijn vastgelegd?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.11.4		Zijn formele procedures opgesteld voor het registreren en afmelden van aangeslotenen voor toegang tot informatiesystemen en -diensten met meerdere gebruikers?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.11.5		Worden speciale bevoegdheden aan de hand van formele autorisatieprocedures verleend?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.11.6		Is er een formeel proces ingericht voor de toewijzing van wachtwoorden aan medewerkers van de netwerkorganisatie?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.11.7		Is er een formeel proces ingericht voor de toewijzing van wachtwoorden aan de aangeslotenen	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.11.8		Worden de uitgegeven toegangsrechten van de medewerkers van de ICT-organisatie regelmatig gecontroleerd?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.11.9		Worden de uitgegeven toegangsrechten van de aangeslotenen regelmatig gecontroleerd?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.11.10		Worden de aangeslotenen verplicht om de beveiligingsregels ten aanzien van het kiezen en gebruiken van wachtwoorden in acht te nemen?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd

			o Weet niet
2.11.11		Zorgen de medewerkers ervoor dat onbeheerde apparatuur voldoende is beveiligd?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.11.12		Is een beleid geformuleerd ten aanzien van het gebruik van netwerken en netwerkdiensten?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.11.13		Wordt de route van het werkstation naar de servers beheerst?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.11.14		Kan op afstand op de systemen van de ICT-organisatie worden ingelogd (door medewerkers of 'derden' zoals leveranciers)?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.11.15		Is de toegang van de aangeslotenen op afstand via externe verbindingen beveiligd door middel van een authenticatieprocedure?	G Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.11.16		Verloopt de toegang door de medewerkers van de netwerkorganisatie tot informatiediensten via een veilig aanlogproces?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.11.17		Worden verbindingen die door computersystemen op afstand tot stand worden gebracht, geauthenticeerd?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.11.18		Zijn beveiligingsmaatregelen getroffen voor de beheersing van de toegang tot diagnosepoorten?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.11.19		Zijn grote netwerken opgesplitst in afzonderlijke domeinen?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.11.20		Zijn maatregelen getroffen voor de beperking van de verbindingsmogelijkheden voor de aangeslotenen teneinde de toegangsvereisten voor bepaalde bedrijfstoepassingen te ondersteunen?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.11.21		Zijn in gemeenschappelijke netwerken beveiligingsmaatregelen voor netwerkroutering getroffen?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.11.22		Heeft de netwerkleverancier een duidelijke beschrijving gegeven van alle beveiligingskenmerken van de gebruikte netwerkservices?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd

			○ Weet niet
2.11.23		Wordt een automatisch identificatiesysteem voor werkstations gebruikt om de verbindingen met specifieke locaties en mobiele apparatuur te verifiëren?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.11.24		Verloopt de toegang door de aangeslotenen tot informatiediensten via een veilig aanlogproces?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.11.25		Zijn alle computeractiviteiten tot een individuele aangeslotene terug te voeren?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.11.26		Wordt gebruik gemaakt van een effectief en interactief wachtwoordmanagementsysteem?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.11.27		Zijn maatregelen getroffen voor de beheersing van het gebruik van systeemhulpmiddelen	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.11.28		Is voor alle medewerkers van de organisatie, die de kans lopen het doelwit van dwang of bedreiging te worden, een stil alarm ingevoerd?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.11.29		Is voor inactieve werkstations op locaties met verhoogd risico een time-out voorziening ingesteld?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.11.30		Is de verbindingstijd door de aangeslotenen voor toepassingen met een verhoogd risico beperkt?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.11.31		Worden bepaalde gevoelige toepassingssystemen in een vast toegewezen (geïsoleerde) computeromgeving uitgevoerd?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.11.32		Wordt ergens bijgehouden (in een log bestand van de software) wie wat gedaan heeft op het informatiesysteem?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.11.33		Zijn procedures voor de monitoring van systeemgebruik vastgesteld?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.11.34		Worden systeemklokken gesynchroniseerd teneinde (log)gegevens nauwkeurig te kunnen vastleggen?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet

2.11.35		Is een formeel beleid opgesteld voor de omgang met mobiele systemen welke de risico's behandelt van het werken met mobiele computervoorzieningen?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.11.36		Beschikt de organisatie over een beleid, procedures en normen voor de beheersing van activiteiten op het gebied van telewerken?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet

Aanschaf, ontwikkeling en onderhoud van systemen

Nr.	Sub	Interviewvraag	Antwoordsysteem
2.12.1		Wordt een analyse van de beveiligingseisen uitgevoerd tijdens het specificeren van de eisen voor een te ontwikkelen informatiesysteem?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.12.2		Worden gegevens die worden ingevoerd in toepassingssystemen gevalideerd op juistheid en geschiktheid?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.12.3		Zijn maatregelen getroffen voor de validatie van de interne gegevensverwerking?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.12.4		Wordt authenticatie van berichten toegepast voor toepassingen waarbij de bescherming van de inhoud van berichten essentieel is?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.12.5		Worden controles uitgevoerd op de uitvoergegevens om te verifiëren of de verwerking van de opgeslagen gegevens juist is verlopen?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.12.6		Is een beleid aanwezig voor het gebruik van cryptografische technieken voor de beveiliging van gegevens?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.12.7		Wordt versleuteling toegepast voor de bescherming van gevoelige informatie?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.12.8		Wordt voor de waarborging van de authenticiteit en de integriteit van elektronische documenten gebruik gemaakt van digitale handtekeningen?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.12.9		Wordt gebruik gemaakt van diensten die de onweerlegbaarheid kunnen aantonen van gebeurtenissen, om eventuele meningsverschillen uit de weg te ruimen over het bestaan van deze gebeurtenissen?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.12.10		Is een managementsysteem aanwezig voor het beheer van cryptografische sleutels?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen)

			○ Altijd ○ Weet niet
2.12.11		Wordt de implementatie van software op operationele systemen nauwkeurig beheerst?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.12.12		Zijn maatregelen getroffen voor de beveiliging en het beheer van testgegevens?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.12.13		Zijn maatregelen getroffen voor de toegangsbeveiliging van softwarebibliotheken?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.12.14		Zijn formele procedures opgesteld voor het beheer van wijzigingen in informatiesystemen?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.12.15		Worden de gevolgen voor de beveiliging van alle wijzigingen in het besturingssysteem nagegaan?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.12.16		Worden wijzigingen in softwarepakketten zoveel mogelijk vermeden?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.12.17		Zijn maatregelen getroffen ter voorkoming van de opname van Trojaanse paarden en geheime communicatiekanalen in informatiesystemen?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.12.18		Is een beleid geformuleerd voor het uitbesteden van de ontwikkeling van programmatuur?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet

Continuïteitsbeheer

Nr.	Sub	Interviewvraag	Antwoordsysteem
2.13.1		Is een proces ingericht voor het ontwikkelen en handhaven van de bedrijfscontinuïteit?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.13.2		Is een risicoanalyse uitgevoerd waarbij gebeurtenissen zijn geïdentificeerd die de continuïteit van de bedrijfsprocessen in gevaar kunnen brengen en waarbij de gevolgen van onderbrekingen voor de bedrijfsprocessen zijn vastgesteld?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.13.3		Zijn continuïteitsplannen opgesteld voor het in stand houden of herstellen van de bedrijfsactiviteiten na een onderbreking of verstoring van het bedrijfsproces?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.13.4		Wordt (via SLA) de beschikbaarheid van de netwerkinfrastructuur vastgelegd?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit

			○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.13.5		Zijn er voorzieningen getroffen om in geval van nood (brand, ontploffing) het netwerk beschikbaar te houden voor de aangeslotenen (b.v. via een uitwijklocatie en vervanging apparatuur)?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.13.6		Worden continuïteitsplannen regelmatig getest, onderhouden en geëvalueerd?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet

Naleving

Nr.	Sub	Interviewvraag	Antwoordsysteem
2.14.1		Is binnen de netwerkorganisatie bekend aan welke wetgeving, naast de WBP, allemaal voldaan moet worden?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.14.2		Wordt binnen de netwerkorganisatie periodiek beoordeeld dat conform relevante wetgeving gewerkt wordt?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.14.3		Worden na een evaluatie de afspraken herzien en/of plannen gemaakt om e.e.a. aan te pakken, aan te scherpen?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.14.4		Wordt een overzicht bijgehouden van de van toepassing zijnde wetten en contractuele voorschriften en de bijbehorende specifieke maatregelen en individuele verantwoordelijkheden?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.14.5		Zijn maatregelen genomen om te waarborgen dat wordt voldaan aan wettelijke en contractuele vereisten met betrekking tot het gebruik van materiaal waarop intellectuele eigendomsrechten rusten?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.14.6		Zijn maatregelen geïmplementeerd om belangrijke documenten en informatie tegen verlies, vernietiging en vervalsing te beveiligen en hiermee te voldoen aan wettelijke en zakelijke vereisten?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.14.7		Zijn maatregelen getroffen om de naleving van privacywetgeving te waarborgen?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.14.8		Zijn maatregelen genomen om ervoor te zorgen dat informatieverwerkende voorzieningen van de netwerkorganisatie alleen voor geautoriseerde organisatiedoeleinden worden gebruikt?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet
2.14.9		Zijn procedures opgesteld om ervan verzekerd te zijn dat afspraken, wettelijke en contractuele vereisten met betrekking tot het gebruik van cryptografische middelen worden nagekomen?	Gesloten vraag; kies een van deze alternatieven: ○ Nooit ○ Soms (<50% van de gevallen) ○ Meestal (>50% van de gevallen) ○ Altijd ○ Weet niet

2.14.10		Zijn regels aanwezig voor het verzamelen van bewijs dat kan worden gebruikt als ondersteuning bij een actie tegen een bepaalde persoon of organisatie?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.14.11		Wordt regelmatig gecontroleerd en geëvalueerd of alle informatieverwerkende voorzieningen voldoen aan het beveiligingsbeleid, de beveiligingsnormen en andere beveiligingseisen?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.14.12		Worden informatiesystemen regelmatig gecontroleerd op de naleving van technisch beveiligingsnormen?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.14.13		Worden audits van operationele systemen gepland en goedgekeurd teneinde het risico van verstoringen van bedrijfsprocessen tot een minimum te beperken?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.14.14		Wordt de toegang tot hulpmiddelen voor systeemaudits beheerd teneinde misbruik of verminking te voorkomen?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet

Beveiligingsincidenten

Nr.	Sub	Interviewvraag	Antwoordsysteem
2.15.1		Is er een meldingprocedure voor beveiligingsincidenten?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.15.2		Is er een registratieplicht voor systeembeheerders voor alle systeemwerkzaamheden- en verstoringen?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.15.3		Bevatten de gevoerde registraties een overzicht van melding, consequentie en actie?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.15.4		Is er een evaluatie- en verbeterproces voor gemelde incidenten?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet

Bewaartermijnen

Nr.	Sub	Interviewvraag	Antwoordsysteem
2.16.1		Is er voor de beschreven verwerking een (wettelijke) bewaartermijn vastgesteld?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.16.2		Is de gehanteerde bewaartermijn in overeenstemming met de wettelijke regels?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet

2.16.3		Gelden afwijkende termijnen indien de gegevens in niet-herleidbare vorm worden bewaard?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet
2.16.4		Indien er geen wettelijke termijn is vastgesteld, is de gehanteerde bewaartermijn redelijk in combinatie met de voor deze verwerking gestelde doelen?	Gesloten vraag; kies een van deze alternatieven: o Nooit o Soms (<50% van de gevallen) o Meestal (>50% van de gevallen) o Altijd o Weet niet

Bijlage 5: voorbeeld respons quick-scan

-----Oorspronkelijk bericht-----
Van: WBP Quick Scan [mailto:WBP Quick Scan]
Verzonden: maandag 27 december 2004 13:34
Aan: Pol, Stephan van der
Onderwerp: Resultaten WBP Quick Scan

Datum van invullen:	**27.12.04**
Respondent:	**S. van der Pol**
Lokatie / dienst:	**ICT**
Vraag 2.1.0a; transparantie huidig:	**2**
Vraag 2.1.0b; transparantie gewenst:	**4**
Vraag 2.2.0a; doelbinding huidig:	**2**
Vraag 2.2.0b; doelbinding gewenst:	**4**
Vraag 2.3.0a; grondslag huidig:	**1**
Vraag 2.3.0b; grondslag gewenst:	**4**
Vraag 2.4.0a; kwaliteit huidig:	**2**
Vraag 2.4.0b; kwaliteit gewenst:	**4**
Vraag 2.5.0a; beveiliging huidig:	**4**
Vraag 2.5.0b; beveiliging huidig:	**4**
Vraag 2.6.0a; bewaartermijn huidig:	**3**
Vraag 2.6.0b; bewaartermijn gewenst:	**4**
Opmerkingen	**Geen opmerkingen**

Bijlage 6: voorbeeld respons inventarisatie

-----Oorspronkelijk bericht-----
Van: n.van.dongen01@vitalis-zorggroep.nl [mailto:n.van.dongen01@vitalis-zorggroep.nl]
Verzonden: woensdag 12 januari 2005 21:44
Aan: Pol, Stephan van der
Onderwerp: WBP Inventarisatie Verwerkingen

Datum melding:	05.01.12
Naam respondent:	N.C.G. van Dongen
Naam lokatie / dienst:	Theresia
Vraag 1.1: aanspreekpunt van de verwerking:	N . v. Dongen
Vraag 1.2.a: dagelijkse naam van de verwerking:	personalia bewoners
Vraag 1.2.b: Produkten en diensten	0=nee; 1=ja
Voor bewoners: persoonlijke verzorging	1
Voor bewoners: huishoudelijke verzorging	1
Voor bewoners: verpleging	1
Voor bewoners: ondersteunende begeleiding	1
Voor bewoners: activerende begeleiding	0
Voor bewoners: behandeling	1
Voor bewoners: verblijf	1
Voor medewerkers: sollicitanten	0
Voor medewerkers: uitzendkrachten	0
Voor medewerkers: vrijwilligers	0
Voor medewerkers: vast personeel	0
Voor medewerkers: zieke werknemers	0
Voor medewerkers: ex-werknemers	0
Voor medewerkers: OBU-Gepensioneerden	0
Vraag 1.3.a: doelen van de verwerking	worden gebruikt om de zorg en diensten te kunnen verlenen welke de klant van ons wenst te ontvangen
Vraag 1.3.b: grondslagen van de verwerking	0=nee; 1=ja
ondubbelzinnige toestemming	1
(pre) contractuele verplichting	1
wettelijk verplicht	0
gerechtvaardigd belang	0
Vraag 1.4: Betrokkenen	0=nee; 1=ja
patient of bewoner	1
relaties van patient of bewoner	1
externe hulpverleners	1
sollicitanten	0
vast personeel (niet ziek of arbeidsongeschikt)	0
zieke of arbeidsongeschikte personeelsleden	0
uitzendkrachten, inleners en gedetacheerden	0
(actieve) vrijwilligers	0
ex-personeelsleden (niet leeftijdgebonden)	0
gepensioneerden en OBU	0
andere typen	soms een leverancier van een voor de klant specifiek hulpmiddel, de apotheek, het Centraal administratiekantoor i.v.m. de eigen bijdrage en het zorgkantoor.
Vraag 1.5: soorten persoonsgegevens	0=nee; 1=ja
Persoonlijke en/of identificerende	1

gegevens	
Financiele en administratieve gegevens	1
Medische en sociaal-psychologische gegevens	1
Gegevens met betrekking tot ras en etniciteit	0
Gegevens met betrekking tot godsdienst en levensovertuiging	1
Strafrechtelijke gegevens of gegevens die betrekking hebben op onrechtmatig dan wel hinderlijk gedrag	0
Andere soorten of categorien van gegevens:	
Vraag 1.6: bewerker	
Is er een bewerker:	Nee
Zo ja, wie	
Vraag 1.7.a: Gebruikers	medewerkers van locatie en algemene dienst Vitalis: bewonersadministratie
Vraag 1.7.b: Beheerder(s)	leidinggevende: hoofd zorg en interne zaken en / of hoofd zorgteam. Administratieve verwerking gebreurt door medewerkers receptie.
Vraag 1.7.c: Derde(n)	niemand
Vraag 1.8: Herkomst	van betrokkene zelf, vaak via RIO bij indicering, waar ook schriftelijk toestemming gevraagd wordt voor het ruime gebruik van deze gegevens in het kader van het doel: namelijk zorg en dienstverlening kunnen leveren.
Vraag 1.9: Beveiliging	Gegevens zijn alleen op papier aanwezig in zorgdossier, verzamelklapperin kantoor en bij receptie: dit alles niet toegankelijk voor derden.
Vraag 1.10: Buitenlandse doorgiften	Nee
Vraag 1.11: Melding	FG
Vraag 1.12: Werking	Deel gegevens komt digitaal via AZR binnen, ontbrekende gegevens wordt van klant verkregen, geheel wordt ingestuurd naar bewonersadministratie doorgestuurd die het verwerken tot een document: personaliaformulier. Mutaties later worden gemeld bij Bewonersadministtratie en gewijzigd document wordt ontvangen.
E-mailadres respondent	n.van.dongen01@vitalis-zorggroep.nl

Bijlage 7: statistische bewerkingen quick-scan

Schattingsfouten

Statistics

		210a: transparantie huidig	220a: doelbinding huidig	230a: grondslag huidig	240a: kwaliteit huidig	250a: beveiliging huidig	260a: bewaarter mijn huidig
N	Valid	13	13	13	13	13	13
	Missing	0	0	0	0	0	0
Std. Error of Mean		,27	,38	,40	,32	,39	,35
Median		2,00	2,00	2,00	2,00	2,00	3,00

Statistics

		210b: transparantie gewenst	220b: doelbinding gewenst	230b: grondslag gewenst	240b: kwaliteit gewenst	250b: beveiliging gewenst	260b: bewaarter mijn gewenst
N	Valid	13	13	13	13	13	13
	Missing	0	0	0	0	0	0
Std. Error of Mean		,36	,36	,23	,23	,14	,14
Median		4,00	4,00	4,00	4,00	4,00	5,00

Correlatietoetsen

RELIABILITY ANALYSIS - SCALE (ALPHA)

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Alpha if Item Deleted
TRANSHUI	11,3846	29,0897	,4660	,5014	,8677
DOELHUID	11,0000	23,3333	,7465	,5693	,8207
GROHUID	10,9231	26,5769	,4310	,3828	,8828
KWALHUID	11,0000	25,0000	,7434	,6211	,8244
BEVHUID	11,0000	22,0000	,8239	,7955	,8042
BEWHUID	10,8462	23,9744	,7663	,7842	,8182

Reliability Coefficients 6 items
Alpha = ,8618 Standardized item alpha = ,8631

RELIABILITY ANALYSIS - SCALE (ALPHA)

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Alpha if Item Deleted
TRANSGEW	21,3077	11,5641	,3037	.	,8647
DOELGEW	21,4615	10,9359	,3919	.	,8397
GROGEW	21,0769	10,4103	,8930	.	,7050
KWALGEW	21,0769	10,4103	,8930	.	,7050
BEVGEW	20,8462	12,8077	,7595	.	,7658
BEWGEW	20,7692	12,6923	,7941	.	,7614

Reliability Coefficients 6 items
Alpha = ,8052 Standardized item alpha = ,8881

Kruskal-Wallis Test huidige situatie

Test Statistics[a,b]

	2#1#0#a	2#2#0#a	2#3#0#a	2#4#0#a	2#5#0#a	2#6#0#a
Chi-Square	8,472	7,923	12,000	11,336	11,117	7,732
df	9	9	9	9	9	9
Asymp. Sig.	,487	,542	,213	,253	,268	,561

a. Kruskal Wallis Test

b. Grouping Variable: LOKNUM

Median Test huidige situatie

Test Statistics

	2#1#0#a	2#2#0#a	2#3#0#a	2#4#0#a	2#5#0#a	2#6#0#a
N	13	13	13	13	13	13
Median	2,00	2,0000	2,0000	2,0000	2,0000	3,0000
Chi-Square	8,775	9,982	13,000	13,000	13,000	8,775
df	9	9	9	9	9	9
Asymp. Sig.	,458	,352	,163	,163	,163	,458

Kruskal-Wallis Test gewenste situatie

Test Statistics[a,b]

	2#1#0#b	2#2#0#b	2#3#0#b	2#4#0#b	2#5#0#b	2#6#0#b
Chi-Square	8,826	6,257	7,871	7,871	9,214	9,214
df	9	9	9	9	9	9
Asymp. Sig.	,453	,714	,547	,547	,418	,418

a. Kruskal Wallis Test

b. Grouping Variable: LOKNUM

Median Test gewenste situatie

Test Statistics

	2#1#0#b	2#2#0#b	2#3#0#b	2#4#0#b	2#5#0#b	2#6#0#b
N	13	13	13	13	13	13
Median	4,0000	4,0000	4,0000	4,0000	4,0000	5,0000
Chi-Square	9,982	8,775	9,982	9,982	9,982	
df	9	9	9	9	9	
Asymp. Sig.	,352	,458	,352	,352	,352	

Bijlage 8: statistische bewerkingen diepte-interviews

Correlatietoetsen voor organisatie

RELIABILITY ANALYSIS - SCALE (ALPHA)

N of Cases = 4,0

Item Means	Mean	Minimum	Maximum	Range	Max/Min	Variance
	2,7224	1,2500	4,7500	3,5000	3,8000	,9221

Reliability Coefficients 172 items
Alpha = ,7012 Standardized item alpha = ,7412

Uitkomsten per indicator voor de organisatie

Statistics

	N		
	Valid	Missing	Median
Transparantie	4	0	3,00
Doelbinding	4	0	3,00
Rechtmatige grondslag	4	0	2,50
Kwaliteit	4	0	4,00
Beveiliging totaal	4	0	3,50
Beveiligingsbeleid	4	0	4,00
Organiseren van informatiebeveiliging	0	4	
Beheer van middelen	0	4	
Beveiliging tav personeel	4	0	2,00
Fysieke beveiliging	0	4	
Operationeel beheer	0	4	
Toegangsbeveiliging	0	4	
Aanschaf, ontwikkeling en onderhoud	0	4	
Continuiteitsbeheer	1	3	3,00
Naleving	1	3	3,00
Beveiligingsincidenten	1	3	4,00
Bewaartermijnen	4	0	4,00

Uitkomsten per indicator voor de afdeling ICT

Statistics

	N		
	Valid	Missing	Median
Transparantie	5	0	3,00
Doelbinding	5	0	1,00
Rechtmatige grondslag	5	0	2,00
Kwaliteit	5	0	4,00
Beveiliging totaal	5	0	3,00
Beveiligingsbeleid	5	0	3,00
Organiseren van informatiebeveiliging	5	0	1,00
Beheer van middelen	5	0	3,00
Beveiliging tav personeel	5	0	2,00
Fysieke beveiliging	5	0	3,00
Operationeel beheer	5	0	4,00
Toegangsbeveiliging	5	0	4,00
Aanschaf, ontwikkeling en onderhoud	5	0	3,00
Continuiteitsbeheer	5	0	2,00
Naleving	5	0	2,00
Beveiligingsincidenten	5	0	3,00
Bewaartermijnen	5	0	1,00

Non Parametric Tests op de separate indicatoren

Mann-Whitney Test

Ranks

	Afdelingsnummer	N	Mean Rank	Sum of Ranks
Transparantie	Afdeling ICT	5	4,40	22,00
	Rest van de organisatie	4	5,75	23,00
	Total	9		
Doelbinding	Afdeling ICT	5	3,90	19,50
	Rest van de organisatie	4	6,38	25,50
	Total	9		
Rechtmatige grondslag	Afdeling ICT	5	4,80	24,00
	Rest van de organisatie	4	5,25	21,00
	Total	9		
Kwaliteit	Afdeling ICT	5	4,40	22,00
	Rest van de organisatie	4	5,75	23,00
	Total	9		
Beveiliging totaal	Afdeling ICT	5	4,10	20,50
	Rest van de organisatie	4	6,13	24,50
	Total	9		
Bewaartermijnen	Afdeling ICT	5	3,00	15,00
	Rest van de organisatie	4	7,50	30,00
	Total	9		

Test Statistics[b]

	Transparantie	Doelbinding	Rechtmatige grondslag	Kwaliteit	Beveiliging totaal	Bewaartermijnen
Mann-Whitney U	7,000	4,500	9,000	7,000	5,500	,000
Wilcoxon W	22,000	19,500	24,000	22,000	20,500	15,000
Z	-,764	-1,433	-,283	-,822	-1,178	-2,570
Asymp. Sig. (2-tailed)	,445	,152	,777	,411	,239	,010
Exact Sig. [2*(1-tailed Sig.)]	,556[a]	,190[a]	,905[a]	,556[a]	,286[a]	,016[a]

a. Not corrected for ties.

b. Grouping Variable: Afdelingsnummer

Two-Sample Kolmogorov-Smirnov Test

Frequencies

	Afdelingsnummer	N
Transparantie	Afdeling ICT	5
	Rest van de organisatie	4
	Total	9
Doelbinding	Afdeling ICT	5
	Rest van de organisatie	4
	Total	9
Rechtmatige grondslag	Afdeling ICT	5
	Rest van de organisatie	4
	Total	9
Kwaliteit	Afdeling ICT	5
	Rest van de organisatie	4
	Total	9
Beveiliging totaal	Afdeling ICT	5
	Rest van de organisatie	4
	Total	9
Bewaartermijnen	Afdeling ICT	5
	Rest van de organisatie	4
	Total	9

Test Statistics[a]

		Transparantie	Doelbinding	Rechtmatige grondslag	Kwaliteit	Beveiliging totaal	Bewaartermijnen
Most Extreme Differences	Absolute	,500	,550	,100	,250	,500	1,000
	Positive	,500	,550	,100	,250	,500	1,000
	Negative	-,100	,000	,000	,000	,000	,000
Kolmogorov-Smirnov Z		,745	,820	,149	,373	,745	1,491
Asymp. Sig. (2-tailed)		,635	,512	1,000	,999	,635	,023

a. Grouping Variable: Afdelingsnummer

Non Parametric Tests op de theoretische variabele "voldoet aan de WBP"

Mann-Whitney Test

Ranks

	Afdelingsnummer	N	Mean Rank	Sum of Ranks
VOLDOET	Afdeling ICT	5	4,10	20,50
	Rest van de organisatie	4	6,13	24,50
	Total	9		

Test Statistics[b]

	VOLDOET
Mann-Whitney U	5,500
Wilcoxon W	20,500
Z	-1,178
Asymp. Sig. (2-tailed)	,239
Exact Sig. [2*(1-tailed Sig.)]	,286[a]

a. Not corrected for ties.

b. Grouping Variable: Afdelingsnummer

Two-Sample Kolmogorov-Smirnov Test

Frequencies

	Afdelingsnummer	N
VOLDOET	Afdeling ICT	5
	Rest van de organisatie	4
	Total	9

Test Statistics[a]

		VOLDOET
Most Extreme Differences	Absolute	,500
	Positive	,500
	Negative	,000
Kolmogorov-Smirnov Z		,745
Asymp. Sig. (2-tailed)		,635

a. Grouping Variable: Afdelingsnummer