Bijlage 3

Aanpak van Privacybescherming

Langdurige Zorg

Inhoudsopgave

1 Inleiding privacybescherming

Om goed met de regels rond privacybescherming uit de voeten te kunnen is het van belang vast te stellen wat er onder privacy kan worden verstaan en wat deze regels inhouden. In dit hoofdstuk wordt een introductie gegeven van de regels rond privacybescherming.

1.1 Wat is privacybescherming?

Het recht op privacy betekent het recht om controle te houden over je eigen persoonsgegevens *(the right to know what other people know about you)*. Het belang van privacy neemt met de digitalisering steeds meer toe. Essentie is dat voorkomen moet worden dat een inbreuk wordt gemaakt op de persoonlijke levenssfeer en wanneer een inbreuk noodzakelijk is, moet deze voorzien worden van een aantal effectieve waarborgen.

Het op dit moment geldende privacyrecht wordt met name bepaald door de Wbp. Daarnaast kennen verschillende sectorale wetten privacybepalingen, die soms in de plaats komen van die van de Wbp en soms aanvullend zijn ten opzichte van de Wbp. Voorbeelden van de eerste categorie zijn de Wet politiegegevens en de Wet gemeentelijke basisadministratie. Voorbeelden van de tweede categorie zijn de Wet geneeskundige behandelingsovereenkomst (Wgbo) en de Wet op de jeugdhulpverlening. De Wbp vloeit voort uit de Europese privacyrichtlijn.[1] De voorgestelde Europese privacyverordening (Epv) komt straks in de plaats van de Europese richtlijn.[2] Afronding van de onderhandelingen over de voorgestelde Epv wordt in de loop van 2014 verwacht. De Epv is dan vanaf 2016 volledig van toepassing.

1.2 De beginselen

De privacybescherming regelt de bescherming van gegevens van de natuurlijke persoon. Deze natuurlijke persoon wordt 'betrokkene' genoemd. De tot deze individuele persoon herleidbare gegevens worden persoonsgegevens genoemd. De privacywet- en regelgeving regelt onder welke voorwaarden

[1] Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband niet de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. PbEG 1995 L 281/31.
[2] De privacyverordening hoeft in tegenstelling tot de richtlijn, niet naar Nederlandse wetgeving te worden omgezet (geïmplementeerd) en zal rechtstreeks van toepassing zijn.

deze persoonsgegevens verwerkt mogen worden en eventueel aan anderen verstrekt mogen worden. Uitgangspunt is dat de betrokkene zelf controle kan houden over zijn eigen gegevens. Eén van de beginselen is dan ook het transparantiebeginsel. Alleen als de verantwoordelijke organisatie die zijn persoonsgegevens verwerkt aan de betrokkene meedeelt dat deze zijn gegevens verwerkt en daarbij kenbaar maakt voor welk doel hij dat doet en hoe lang hij zijn gegevens bewaart, is de betrokkene in staat die controle te houden. Andere belangrijke beginselen zijn het doelbindingsbeginsel en de beginselen van proportionaliteit en subsidiariteit. Met doelbindingsbeginsel wordt bedoeld dat gegevens slechts mogen worden verwerkt voor een van te voren welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doeleinde. Met het proportionaliteitsbeginsel (ook wel evenredigheidsbeginsel genoemd) wordt bedoeld dat de inbreuk op de belangen van de bij de verwerking van persoonsgegevens betrokkene niet onevenredig mag zijn in verhouding tot het met de verwerking te dienen doel. Het subsidiariteitsbeginsel houdt in dat het doel waarvoor de persoonsgegevens worden verwerkt in redelijkheid niet op een andere voor de betrokkene minder nadelige wijze kan worden bereikt.

1.2.1 Begrippen

Binnen de privacywet- en regelgeving worden specifieke begrippen gehanteerd. Tussen de Wbp en de Epv zitten hierin verschillen. Zo introduceert de Epv enkele nieuwe begrippen (zoals genetische gegevens) maar zijn ook een paar begrippen gewijzigd (de bewerker wordt in de Epv nu verwerker genoemd). Gezien het feit dat de Epv binnenkort van toepassing wordt, zetten we hier de belangrijkste begrippen zoals ze voorkomen in de Epv op een rij:[3]

- *Betrokkene* Het gaat hier om degene waarvan de persoonsgegevens worden verwerkt. Een natuurlijk persoon die geïdentificeerd is of geïdentificeerd kan worden. Het laatste kan onder andere aan de hand van een identificatienummer, gegevens over de verblijfplaats van de persoon, een online-identificatiemiddel of een of meer specifieke elementen die kenmerkend zijn voor zijn fysieke, fysiologische, genetische, mentale, economische, culturele of sociale identiteit.

- *Verwerking* Het komt erop neer dat elke bewerking van persoonsgegevens – geautomatiseerd of niet – hieronder valt. Enkele voorbeelden zijn het verzamelen, wijzigen, bijwerken, ordenen,

[3] Voor een letterlijke omschrijving van de begrippen verwijzen we naar artikel 4 van de voorgestelde Epv.

raadplegen, ter beschikkingstellen, met elkaar in verband brengen, wissen of vernietigen van gegevens.

- *Bestand* Dit begrip is gedefinieerd omdat het hebben van een bestand maakt dat een niet-geautomatiseerde verwerking die geen bestand is hiermee geen verwerking is die onder de werking van de voorgestelde privacyverordening valt. Bij een bestand moet men denken aan een gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd dan wel gedecentraliseerd is of verspreid op een functioneel of geografisch bepaalde wijze.

- *Verantwoordelijke (voor de verwerking)* De natuurlijke of rechtspersoon, de overheidsinstantie, de dienst of enig ander orgaan dat allen of tezamen met anderen, het doel van en de voorwaarden en middelen voor de verwerking van persoonsgegevens vaststelt. Bepalend is dat de verantwoordelijke het doel, de voorwaarden en middelen voor verwerking vaststelt.

- *Verwerker* De verwerker is de natuurlijke of rechtspersoon, de overheidsinstantie, die dienst of enig ander orgaan die, respectievelijk dat ten behoeve van de verantwoordelijke persoonsgegevens verwerkt. Voor de verwerker gelden bijna dezelfde verplichtingen als voor de verantwoordelijke.

- *Inbreuk* Dit begrip is van belang in verband met de meldplicht bij datalekken. Het gaat hier op een inbreuk op de beveiliging van persoonsgegevens. Dit moet een gevolg hebben dat een nadeel vormt. Een nadeel zou kunnen zijn: vernietiging, verlies van gegevens of de ongeoorloofde toegang tot gegevens. Een inbreuk hoeft niet onrechtmatig te zijn veroorzaakt maar kan ook per ongeluk gebeuren.

- *Biometrische gegevens* Eenduidige kenmerking gebeurt met deze gegevens aan de hand van bijvoorbeeld afbeeldingen van het gezicht. In de privacyverordening komt dit begrip alleen maar voor in combinatie met de privacyeffectbeoordeling (PIA).

- *Toestemming*: Gewaarborgd moet worden dat de betrokkene zich ervan bewust is dat hij toestemming geeft en waarvoor hij toestemming geeft:

- de verantwoordelijke moet kunnen aantonen dat de betrokkene toestemming heeft gegeven.[4]
- wanneer de betrokkene zijn toestemming moet geven in het kader van een schriftelijke verklaring die ook op een andere gelegenheid betrekking heeft, moet het vereiste van toestemming duidelijk afzonderlijk van deze andere aangelegenheid worden weergegeven.
- de betrokkene heeft het recht zijn toestemming te allen tijde in te trekken.
- toestemming biedt geen rechtsgrondslag voor verwerking wanneer er een aanzienlijke onevenwichtigheid bestaat tussen de positie van de betrokkene en de verantwoordelijke. Van zo'n onevenwichtigheid is bijvoorbeeld sprake in het geval een werkgever persoonsgegevens van een werknemer verwerkt. Dat wil niet zeggen dat het dan niet is toegestaan. Vaak is er een andere gerechtvaardigde grondslag dan toestemming, zoals de nakoming van een wettelijke plicht (aangifte loonheffing) of uitvoering van een overeenkomst (arbeidscontract).

- *Samenwerkingsverbanden*: partners van samenwerkingsverbanden die voor een gezamenlijke verwerking van persoonsgegevens verantwoordelijkheid dragen, moeten dit door middel van een onderlinge regeling (bijvoorbeeld een overeenkomst) vastleggen. Daarin stellen zij hun respectieve verantwoordelijkheden vast voor de nakoming van de verplichtingen die uit de verordening voortvloeien, met name met betrekking tot de procedures en mechanismen voor de uitoefening van de rechten van betrokkenen.

  Dit gaat verder dan wat partners van samenwerkingsverbanden doorgaans gewend zijn. Nu worden ze, naast het overeenkomen van een overeenkomst, verplicht hun procedures en mechanismen uit te werken voor de effectuering van de rechten van betrokkenen en deze op elkaar af te stemmen.

- *Bescherming van het kind*: De bescherming van persoonsgegevens van kinderen speelt met name een rol bij direct marketing en in de gezondheidszorg; iemand is kind tot de persoon achttien jaar oud is. In de privacyverordening wordt aan de privacybescherming van kinderen extra gewicht toegekend.

[4] Zie artikel 7 lid 1 van de voorgestelde privacyverordening.

1.3 Enkele kernbepalingen uitgelicht

1.3.1 Algemene documentatieverplichting

De privacyverordening bevat een algemene documentatieverplichting.[5] Verantwoordelijken en bewerkers alsmede vertegenwoordigers van verantwoordelijken worden verplicht alle documenten te bewaren inzake alle gegevensverwerkingen die onder hun verantwoordelijkheid hebben plaatsgevonden. De documenten bevatten gegevens zoals de naam en contactgegevens van de verantwoordelijke en de eventuele gezamenlijk voor de verwerking verantwoordelijke of verwerker en de eventuele functionaris gegevensbescherming, de doeleinden van de verwerking, waaronder de gerechtvaardigde belangen van de verantwoordelijke wanneer de verwerking op die grondslag is gebaseerd[6] en/of de eventuele wettelijke basis, betrokkenen en categorieën betrokkenen, de ontvangers of categorieën van ontvangers van persoonsgegevens, de bewaartermijn van gegevens etc. De documentatieplicht lijkt op de meldingsplicht zoals we die in de Wbp kennen.

1.3.2 Informatieplicht

De informatieplicht (ten behoeve van de betrokkene) is in de voorgestelde Epv sterk uitgebreid. Naast de verplichting voor de verantwoordelijke om informatie over het doel van de verwerking en de identiteit en contactgegevens van verantwoordelijke en functionaris voor de gegevensbescherming (FG) aan de betrokkenen te verstrekken, zal hij de betrokkene nu ook informatie moeten verstrekken over onder meer de periode gedurende welke de persoonsgegevens worden opgeslagen, het bestaan van het recht op toegang tot en rectificatie of vernietiging van zijn gegevens en het bestaan van het recht om een klacht in te dienen bij het College Bescherming Persoonsgegevens (CBP) en ontvangers van persoonsgegevens. Dit zal hij moeten kunnen aantonen. Bovendien moet de informatie in begrijpelijke vorm en duidelijke en eenvoudig taal worden verstrekt. ‘De betrokkene had kunnen weten …..’ is dus niet meer aan de orde. De commissie LIBE van het Europees parlement heeft voorgesteld dat betrokkenen voorafgaand aan het verstrekken van deze specifieke informatie, het informatiebeleid ter hand wordt gesteld. Aan de hand van dit informatiebeleid moet de betrokkene het privacybeschermingsniveau snel inzichtelijk kunnen krijgen.

[5] Artikel 28 voorgestelde Epv.

[6] Artikel 6 lid 1, sub f voorgestelde Epv.

1.3.3 Rechten van betrokkenen

Om de rechten van betrokkenen zo goed mogelijk te waarborgen worden verantwoordelijken in de voorgestelde Epv verplicht om procedures en mechanismes vast te stellen voor het verstrekken van eerder genoemde informatie en voor het uitoefenen van de rechten van betrokkenen.[7] Als het over rechten van betrokkenen gaat, gaat het met name om:

- het recht van toegang tot zijn gegevens;
- het recht van rectificatie;
- het recht om vergeten te worden;
- het recht om gegevens te laten wissen;
- het recht van gegevensoverdraagbaarheid;
- en het recht van bezwaar.

Nadere toelichting op enkele van de hiervoor genoemde rechten

Het *recht om vergeten te worden* betekent dat de betrokkene een recht heeft op volledige verwijdering van zijn persoonsgegevens indien hij zijn toestemming intrekt en er geen andere legitieme redenen zijn om de data te bewaren. De verantwoordelijke dient derden op de hoogte te stellen van het verzoek van betrokkene om iedere koppeling naar en kopie of reproductie van zijn persoonsgegevens te verwijderen.

De naleving van bewaartermijnen loopt gelijk op met het recht om vergeten te worden. Als de beperkingen die de verplichte bewaartermijnen opleggen niet worden aangehouden, zal het recht om vergeten te worden ook niet worden geëffectueerd.

Het recht van *gegevensoverdraagbaarheid* is een eis die in feite een eis tot standaardisatie is. De betrokkene heeft met dit recht namelijk de mogelijkheid om te vragen dat zijn of haar gegevens worden overgedragen naar een andere partij. Bijvoorbeeld een client stapt over van de ene zorginstelling naar de andere. Daar er al gauw sprake is van een diversiteit aan partijen die hierbij betrokken zijn, is standaardisatie een vereiste om aan dit recht te kunnen voldoen.

[7] Artikel 12 voorgestelde Epv en ook artt. 5d, 14, 17, 18, 19.

1.3.4 Profiling

Iedere betrokkene heeft het recht om niet op basis van profilering aan een maatregel te worden onderworpen waaraan voor hem rechtsgevolgen zijn verbonden of die hem in aanmerkelijke mate treft en die louter wordt genomen op grond van een geautomatiseerde verwerking.[8] Het moet dan gaan om een geautomatiseerde verwerking die bestemd is om bepaalde aspecten van zijn persoonlijkheid te evalueren of om met name zijn beroepsprestaties, economische situatie, verblijfplaats, gezondheid, persoonlijke voorkeuren, betrouwbaarheid of gedrag te analyseren of te voorspellen.

Een persoon mag alleen aan een maatregel, die op basis van profiling tot stand komt, worden onderworpen wanneer de verwerking:

- wordt uitgevoerd in het kader van het sluiten of het uitvoeren van een overeenkomst[9]
- uitdrukkelijk is toegestaan op grond van EU-wetgeving of nationale wetgeving[10]
- plaatsvindt op grond van toestemming van de betrokkene.

1.3.5 Meldplicht datalekken

In geval van een inbreuk in verband met persoonsgegevens is de verantwoordelijke verplicht deze inbreuk of ook wel datalek genoemd binnen 24 uur nadat hij ervan kennis heeft genomen aan het CBP te melden. Hiervan is sprake als bijvoorbeeld hackers in het registratiesysteem binnendringen.[11] De verwerker is verplicht de verantwoordelijke onmiddellijk te waarschuwen en te informeren na vaststelling van een datalek. De verantwoordelijke moet niet alleen aan het CBP melden, de verantwoordelijke moet ook na melding aan het CBP de betrokkene melden.[12] Hij moet dat doen wanneer het waarschijnlijk is dat het datalek negatieve gevolgen heeft voor de bescherming van de persoonsgegevens of de privacy van de betrokkene. En hij moet dat zonder onnodige vertraging doen.

[8] Artikel 20 voorgestelde Epv.

[9] en aan het door de betrokkene ingediende verzoek tot het sluiten of uitvoeren van de overeenkomst is voldaan of passende maatregelen zijn aangeboden ter bescherming van zijn gerechtvaardigde belangen, zoals het recht op menselijke tussenkomst.

[10] en in die wetgeving ook passende maatregelen zijn opgenomen ter bescherming van de gerechtvaardigde belangen van de betrokkene.

[11] Artikel 31 voorgestelde Epv.

[12] Artikel 32 voorgestelde Epv.

1.3.6 Privacy by design en privacy by default (PbD*2)

Nieuw in de privacyverordening zijn de *privacy by design* en *privacy by default* eisen.[13] *Privacy by design* betekent dat al in de voorfase van een (ICT-) project – al vanaf het ontwerp - wordt gekeken naar technische en organisatorische maatregelen die privacyverhogend zijn.[14] In plaats van de wet toe te passen op het te ontwikkelen systeem, wordt de wet in het systeem ingebouwd. *Privacy by design* omvat ook een aan de bouw van systemen, diensten en netwerken voorafgaande privacyrisico- of privacybedreigingsanalyse (*privacy impact analyse*) en een management cyclus binnen organisaties waar privacybescherming een vast onderdeel is.[15] Grosso modo gaat het bij *privacy by design* om het ontwerpen van informatiesystemen, die de privacy van mensen beschermen.

Privacy by default lijkt op het *privacy by design* principe en betekent dat door middel van systeeminstellingen maximale privacy van een betrokkene wordt gewaarborgd en voor zover mogelijk door het systeem wordt afgedwongen.

1.3.7 Privacy Impact Assessment

Een *Privacy Impact Assessment* of ook wel Privacyeffectbeoordeling wordt uitgevoerd wanneer verwerkingen, systemen en ook wetgeving, gezien hun aard, reikwijdte of doeleinden bijzondere risico's inhouden voor de rechten en vrijheden van betrokkenen, voert de verantwoordelijke of bewerker een beoordeling uit van het effect van de beoogde verwerkingen op de bescherming van persoonsgegevens.

1.3.8 Functionaris Gegevensbescherming

De privacyverordening stelt in veel gevallen de aanwijzing van een Functionaris Gegevensbescherming (FG) verplicht. De positie en taken van de FG zijn uitgebreid omschreven.[16] Deze taken zijn onder andere:

[13] Artikel 23 voorgestelde Epv.

[14] Zie de Mededeling van het CBP: 'Privacy by design onontbeerlijk in ICT-tijdperk - CBP-reactie op plan Eurocommissaris Reding voor herziening privacyrichtlijn' dat in november 2010 is gepubliceerd door de CBP http://www.cbpweb.nl/Pages/th_pbd_start.aspx.

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

[16] Artikel 37 voorgestelde Epv.

- het informeren en adviseren van de verantwoordelijke en de verwerker over de verplichting die zij hebben op grond van deze verordening en het documenteren van deze activiteit en de ontvangen antwoorden.
- het toezien op de uitvoering en toepassing van het privacybeleid van de verantwoordelijke of de verwerker, met inbegrip van de toewijzing van verantwoordelijkheden, opleiding van het bij de verwerking betrokken personeel en de audits.
- het toezien op de uitvoering en toepassing van deze verordening, met name ten aanzien van privacy by design, privacy by default en gegevensbeveiliging, de informatieplicht en de effectuering van rechten van betrokkenen.
- ervoor zorgen dat de documenten die voortvloeien uit de eerder genoemde documentatieplicht worden bewaard.
- het toezien op het naleven van de meldplicht datalekken.
- het toezien op de uitvoering van de PIA en op het verzoek om voorafgaande toestemming of raadpleging.

1.3.9 Privacybeleid

Met (intern) privacybeleid wordt bedoeld het beleid dat de verantwoordelijke moet hanteren en handhaven om te voldoen aan de doorlopende eisen die voortvloeien uit de voorgestelde privacyverordening en andere geldende privacywet- en regelgeving. Daarnaast moet de verantwoordelijke passende maatregelen uitvoeren om ervoor te zorgen en te kunnen aantonen dat de verwerkingen in overeenstemming de verordening worden uitgevoerd.

2 Privacybescherming voor de langdurige zorg

In de zorg worden veelvuldig bijzondere persoonsgegevens verwerkt en uitgewisseld. Dit betekent dus dat voor vrijwel alle verwerkingen en uitwisselingen van persoonsgegevens het hoogste niveau van privacybescherming is vereist. Dat is helder maar wat betekent dit nu concreet? Om dit te kunnen duiden worden enkele binnen de zorg van toepassing zijnde normen toegelicht.

Allereerst zijn de beveiligingseisen specifiek voor de zorg aangescherpt in de NEN 7510.[17] De NEN 7510 richt zich op zorginstellingen en andere organisaties die bij informatievoorziening in de gezondheidszorg zijn betrokken, ongeacht de aard en de omvang van het bedrijfsproces. De norm NEN 7510 gaat over informatiebeveiliging binnen de zorgsector. Onder informatiebeveiliging in de zorg wordt verstaan: het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van alle informatie die benodigd is om patiënten verantwoorde zorg te kunnen bieden. Naast het borgen van deze kwaliteitscriteria vereist deze norm ook dat de informatiebeveiligingsmaatregelen op controleerbare wijze zijn ingericht voordat kan worden gesproken over adequate informatiebeveiliging. De norm kan beschouwd worden als een kader. Binnen dit kader kan elke proceseigenaar de voor zijn/haar proces relevant geachte informatiebeveiliging specificeren, inclusief de daarbij behorende maatregelen.

Naast de NEN 7510 zijn er ook de NEN 7511,[18] NEN 7512 en NEN 7513 (hierna tezamen aangeduid met NEN 751n).[19] Hiervan is de NEN 7512 zeer relevant voor de gegevensuitwisseling; het toepassingsgebied is de elektronische communicatie in de zorg, tussen zorgverleners en zorginstellingen onderling en met patiënten en cliënten, zorgverzekeraars en andere partijen die bij de zorg zijn betrokken. In de eerste plaats richt deze norm zich op de zekerheid die partijen elkaar moeten bieden als voorwaarde voor vertrouwde gegevensuitwisseling. Ten tweede levert deze norm een nadere invulling aan een aantal van de richtlijnen van NEN 7510. Dat betreft dan vooral de aanzet tot risicoclassificatie en de uitwerking van de eisen over identificatie en authenticatie die behoren bij een bepaalde risicoklasse.

[17] De norm NEN 7510 is een door het Nederlands Normalisatie-instituut ontwikkelde norm voor Informatiebeveiliging voor de zorgsector in Nederland. De norm is gebaseerd op de Code voor Informatiebeveiliging (zie http://www.nen.nl).
[18] NEN 7511: Toetsbaar voorschrift voor solopraktijken, samenwerkingsverbanden en grote instellingen.
[19] NEN 7513: Logging - Vastleggen van acties op elektronische patiëntdossiers.

Voorts is de NEN 7521 in ontwikkeling.[20] Deze norm geeft de grondslagen voor de toegang tot de uitwisseling van patiëntgegevens.

Na de introductie van de NEN 751n bleek aanvullende behoefte te bestaan aan objectieve en open landelijke toetsingscriteria om de invoering en naleving van de NEN 751n in de praktijk te ondersteunen, te kunnen toetsen en een instelling desgewenst te accrediteren of te certificeren. Hierop hebben het Nederlands Instituut voor Accreditatie in de Zorg (NIAZ) en de Nederlandse Orde van Register EDP-auditors (NOREA) het initiatief genomen om een Toetsingskader voor de Informatieveiligheid in de Zorg te ontwikkelen onder de naam ZekereZorg3. In de toetsingscriteria zijn elementen opgenomen die relevant zijn voor het gebruik van medische apparatuur en patiëntveiligheid. Tevens zijn de wet- en regelgeving die van toepassing zijn op de informatiebeveiliging in de zorg uitgewerkt en worden extra toelichtingen verstrekt voor de toetsingscriteria die van toepassing zijn op de interne en externe uitbesteding van ICT diensten.

Het belang van privacybescherming in de zorg wordt onderstreept door de recentelijk gepubliceerde concept Algemene Maatregel van Bestuur (AMvB) 'Besluit houdende nadere regels over functionele, technische en organisatorische gegevensverwerking door en tussen zorgaanbieders (Besluit elektronische gegevensuitwisseling tussen zorgaanbieders)'.[21] Hierin wordt in meerdere artikelen dwingend verwezen naar de naleving van de NEN 7510, NEN 7512, NEN 7513.

In dit hoofdstuk wordt aan de hand van de in hoofdstuk 2 geschetste kernbepalingen van de privacywetgeving de impact van privacybescherming op de gegevensuitwisseling in de (langdurige) zorg[22] beschreven.

2.1 Betekenis van de privacy kernbepalingen voor de langdurige zorg

De kernbepalingen van de privacywetgeving, zoals die in het vorige hoofdstuk zijn toegelicht worden in dit hoofdstuk nader uitgewerkt voor de gegevensuitwisseling binnen de langdurige zorg. Hierbij wordt

[20] NEN 7521: Medische informatica - Toegang tot en uitwisseling van patiëntgegevens, Concept.

[21] Concept Algemene Maatregel van Bestuur bij de Nota van Wijziging van de Wet cliëntenrechten zorg, de Wet gebruik burgerservicenummer in de zorg, de Wet marktordening gezondheidszorg en de Zorgverzekeringswet (cliëntenrechten bij elektronische verwerking van gegevens), Kamerstukken II 33509, nr. 7, d.d. 19 november 2013. Met de AMvB wordt invulling gegeven aan artikel 26 Wbp door specifieke eisen te stellen voor de zorg.

[22] In beginsel is er geen onderscheid in de eisen en uitwerking van privacybescherming voor de korte en langdurige zorg.

een algemene leidraad gegeven op welke wijze in meer of mindere mate invulling kan worden gegeven aan deze eisen ten aanzien van privacybescherming.

2.1.1 Algemene documentatieverplichting

De algemene documentatieverplichting vereist overzicht en inzicht in de wijze waarop invulling wordt gegeven aan de privacybescherming. Dit betekent dat de verantwoordelijken binnen een organisatie moeten weten welke verwerkingen binnen de organisatie worden gevoerd (of door andere partijen ten behoeve van de organisatie) met alle karakteristieken daarvan, welke personen welke rollen hebben, indien een FG is benoemd wie dat is, met welke partijen welke gegevenssets worden uitgewisseld, etc. Ook moeten de verwerkingen gerelateerd worden aan de informatiesystemen en processen.
Als elke partij binnen de langdurige zorg een dergelijke registratie voert, kunnen ook de onderlinge verbanden worden gesignaleerd en dus de eventuele discrepanties.[23]
Voor de gegevensuitwisseling zelf betekent deze documentatieverplichting ook dat alle aspecten van de gegevensuitwisseling moet worden vastgelegd. Een taxonomie voor de (langdurige) zorg (hierna LZ taxonomie) helpt hier zondermeer bij doordat de gegevenssets die worden uitgewisseld, zijn vastgelegd. Door bovendien een Legal Entity Framework (LEF) te beheren van alle betrokken partijen worden ook de onderlinge verbanden in kaart gebracht.[24]
Daarnaast zal het gebruik van authenticatie, autorisatie en logging tijdens de gegevensuitwisseling inzage geven in wat aan wie is verstrekt onder welke condities. Dit laatste, de condities waaronder gegevens worden uitgewisseld en wat de ontvanger wel of juist niet met de gegevens kan doen, kan worden vorm gegeven door gebruik te maken van zogeheten ‘sticky policies’. Deze worden aan de feitelijke uitwisseling gekoppeld (sticky) en beschrijven op een uniforme wijze de condities (inclusief de gegevens betreffende de betrokken partijen in de gegevensuitwisseling).

2.1.2 Informatieplicht

De informatieplicht aan de betrokkene brengt met zich mee dat de betrokkene ook geïnformeerd moet worden als zijn of haar gegevens worden uitgewisseld. De betrokkene moet immers worden

[23] Duthler Associates heeft taxonomiegedreven tooling ontwikkeld om een dergelijke administratie te voeren, DNA Privacy. Door het open karakter van de registratie kunnen de registraties met elkaar worden gematched en kan bijvoorbeeld worden geconstateerd dat een gegevensuitwisseling wel door de ene partij wordt verzonden maar door de andere partij niet ontvangen.

[24] Zie ook § 2.2.3 en § 3.1.3 van het excerpt van de rapportage ‘Gegevensuitwisseling Langdurige Zorg, De toepassing van gegevenstaxonomieën’ in bijlage X.

geïnformeerd over de ontvangers en categorieën van ontvangers. Deze verplichting geldt ook als het vanzelfsprekend is dat bepaalde gegevens worden gedeeld, denk daarbij bijvoorbeeld aan het declareren bij de zorgverzekeraar.
De uitvoering van de informatieplicht kan op verschillende manieren worden ingericht. Op het moment dat de rechtmatigheidsgrondslag van een verwerking de toestemming van de betrokkene is, kan het moment waarop deze toestemming wordt gevraagd samenvallen met het moment waarop deze toestemming wordt gegeven. Als de verwerking plaatsvindt op grond van de Wet geneeskundige behandelingsovereenkomst (Wgbo) zal dat moment bijna altijd samenvallen.

2.1.3 Rechten van betrokkenen

De rechten van betrokkenen zijn er vooral op gericht dat de betrokkene controle houdt over zijn eigen gegevens. Dat hij of zij inzage heeft in zijn of haar gegevens, vermeende fouten kan laten corrigeren, gegevens kan laten verwijderen en de gegevens naar een andere partij kan laten overdragen.
Ook in een aantal zorgspecifieke wetten wordt aandacht besteed aan deze rechten van betrokken. Dit zijn onder andere de Wgbo met het inzagerecht en het verwijderrecht en de op stapel staande Wet cliëntenrechten in de zorg waarvan de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg[25] onderdeel uitmaakt. In het laatstgenoemde wetsvoorstel wordt de cliënt in geval zijn gegevens elektronisch worden uitgewisseld de mogelijkheid geboden om generieke, beperkte of geen toestemming voor de gegevensuitwisseling te geven, in te trekken of te wijzigen. In geval van generieke toestemming geeft de cliënt toestemming voor het elektronisch ter beschikking stellen van zijn gegevens aan zijn behandelend zorgaanbieder en alle andere zorgaanbieders die zijn aangesloten op het elektronisch uitwisselingssysteem waarmee de cliënt nu of in de toekomst een behandelrelatie mee heeft.[26] In geval cliënt geen toestemming geeft is elektronische uitwisseling in het geheel niet mogelijk. Als cliënt beperkte toestemming worden bepaalde zorgaanbieders of categorieën van zorgaanbieders van de elektronische gegevensuitwisseling op voorhand uitgesloten. Systemen zullen technisch in staat moeten zijn om dit recht te kunnen realiseren. Voor toegang tot en uitwisseling van patiëntgegevens is een norm in ontwikkeling, te weten de NEN 7521. Voorts is er ook de Gedragscode Elektronische

[25] Dit is de nieuwe citeertitel voor de huidige Wet gebruik burgerservicenummer in de zorg (Wbsn-z) zoals deze met de Wijziging van de cliëntenrechten bij elektronische verwerking van gegevens van toepassing wordt.
[26] Zie Kamerstukken II, 33.509, nr. 7. Bijzonder is dat de Nota naar aanleiding van het verslag spreekt van een behandelrelatie met een systeem. Terwijl de Wgbo altijd uitgaat van een behandelrelatie met een hulpverlener.

Gegevensuitwisseling in de Zorg (EGiZ)[27] die een concrete uitwerking vormt van de toepasselijke relevante wet- en regelgeving.

Een aandachtspunt bij het bepalen van de gegevens die onderdeel zijn van het cliëntdossier is de scheiding tussen de gegevens van en over de cliënt en de gegevens van en over de medicus. Laatstgenoemde gegevens kunnen in bepaalde gevallen worden beschouwd als persoonlijke aantekeningen van de medicus en zijn dan formeel gezien geen onderdeel van het cliëntdossier. Dit kan gevolgen hebben voor het effectueren van de rechten van de betrokkene.

Om zijn of haar rechten te kunnen uitoefenen moet de betrokkene weten:

1. Waar welke gegevens worden vastgelegd cq. met wie ze (kunnen) worden uitgewisseld (en dus ook aldaar vastgelegd worden).
2. Wie verantwoordelijke is voor de gegevensverwerking.
3. Welke procedures moeten worden gevolgd om de rechten uit te oefenen.

Om te kunnen voldoen aan de rechten van de betrokkenen is allereerst transparantie vereist. Dat is, gezien het groot aantal partijen dat een rol speelt in de langdurige zorg, een uitdaging op zich. Om het voor de betrokkenen overzichtelijk te houden is het ook wenselijk dat de te volgen procedures bij de partijen in de zorg min of meer uniform zijn en aansluiten. Daarnaast vereist het efficiënt en kosteneffectief invullen van het recht op overdraagbaarheid van gegevens standaardisatie van zowel de gegevenssets als van de wijze waarop de gegevens kunnen worden uitgewisseld. Het project GuStan is bij uitstek geschikt vanuit haar centrale rol om hieraan invulling te geven. Enerzijds door de voorbeeldprocedures te ontwikkelen, anderzijds met het gebruik van de LZ taxonomie en de technische infrastructuur voor de gegevensuitwisseling.

2.1.4 Profiling

De gegevensuitwisseling in de langdurige zorg is vooral gericht op het delen van informatie over de personen die zorg ontvangen (of ondergaan). Het is echter niet uitgesloten dat deze gegevens toch op

[27] Zie bijvoorbeeld http://knmg.artsennet.nl/Publicaties/KNMGpublicatie/Gedragscode-Elektronische-Gegevensuitwisseling-in-de-Zorg-EGiZ-2013..htm.

de een of andere manier worden gebruikt voor andere doeleinden, bijvoorbeeld om vanuit een doelgroep voor een bepaalde behandelmethode een selectie te maken van personen die aan een onderzoek mee mogen doen. Wanneer persoonsgegevens zonder menselijke tussenkomst worden gebruikt voor de selectie is sprake van profiling en dit is niet zonder meer toegestaan. Toestemming van de betrokkene moetdan worden ingebouwd volgens de uitgangspunten van PbD*2. Zie paragraaf 1.3.4 en paragraaf 1.3.6.

2.1.5 Meldplicht datalekken

Daar waar gegevens worden verwerkt en uitgewisseld zal het ook kunnen voorkomen dat ingebroken wordt in informatiesystemen of persoonsgegevens op een andere manier worden onderschept. Als er sprake is van een inbreuk in verband met persoonsgegevens – dat noemen we ook wel een datalek - dan moet dat onverwijld en uiterlijk binnen 24 uur worden gemeld bij het CBP. Als de inbreuk mogelijk negatieve consequenties heeft voor de gegevensbescherming en privacy van betrokkenen moeten deze betrokkenen ook onverwijld worden geïnformeerd. Elke organisatie is verplicht om invulling te geven aan de meldplicht datalekken en zal dus moeten beschikken over een responseplan, inclusief draaiboeken en procedures, om zo'n datalek conform de wettelijke eisen af te handelen: tijdig, volledig en aantoonbaar.

Is er sprake van een inbreuk op de elektronische gegevensuitwisseling of anderszins van een datalek dan zijn er meerdere partijen betrokken en verantwoordelijk om aan deze meldplicht te voldoen. Het is noodzakelijk dat er goede onderlinge afspraken worden gemaakt: welke partij vervult welke rol niet alleen per betrokken organisatie (zorgverzekeraar, zorgaanbieder of zorginstelling), maar ook binnen deze organisaties (directie, ict-afdeling, juristen en communicatie); kunnen betrokkenen op zo'n korte termijn worden geïnformeerd, zijn de contactgegevens van deze betrokkenen op zo'n korte termijn bekend, etc. Ook is het belangrijk responseplannen en 'datalek emergencyteams' op elkaar af te stemmen.

Ook hier zal de centrale regierol van het ministerie van VWS onontbeerlijk zijn. Allereerst door het opstellen van beleid en richtlijnen inzake de uitvoering van de meldplicht. Daarnaast zullen mogelijk andere partijen zoals de Inspectie voor de gezondheidszorg, in de voorkomende gevallen een bepaalde rol moeten spelen. Privacybescherming in de zorg is zowel het toezichtsdomein van het College bescherming persoonsgegevens (CBP) als van de Inspectie voor de Gezondheidszorg (IGZ). Tussen deze

toezichthouders bestaat een samenwerkingsprotocol. Het is dan ook aannemelijk dat IGZ in het kader van de meldplicht datalekken een rol gaat spelen.

2.1.6 Privacy by design en privacy by default

Het project GuStan zal rekening moeten houden met de verplichtingen van privacy by design en privacy by default (PbD*2). Zij zal er dus voor moeten zorgen dat de privacybescherming vanaf het begin onderdeel is van de eisen die gesteld worden aan de resultaten die door het project worden opgeleverd en ook dat het privacy by default-principe is ingebed in de resultaten. Eén van de randvoorwaarden voor de infrastructuur die gebruikt zal worden voor de elektronische gegevensuitwisseling is dat de infrastructuur zal moeten voldoen aan de principes van privacy by design en default.
Daarnaast kunnen de richtlijnen die worden gehanteerd binnen het project GuStan ook worden gedeeld met andere partijen (in de zorg). Hetzelfde geldt voor andere resultaten op dit gebied: denk bijvoorbeeld aan een methode om de gegevens te de-personaliseren of andere PET-technologieën.

2.1.7 Privacy Impact Assessment

Met de voorgestelde Epv en het toetskader PIA's rijksdienst wordt het uitvoeren van PIA's verplicht voor verwerkingen waarmee veel of bijzondere persoonsgegevens – zoals gezondheidsgegevens - zijn gemoeid. Dit geldt dus ook voor elektronische gegevensuitwisselingen. Een PIA resulteert in ieder geval in een algemene beschrijving van de beoogde verwerkingen, een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen, de maatregelen die worden beoogd om de risico's te beperken, en de waarborgen, beveiligingsmaatregelen en mechanismen die de privacybescherming verzekeren en aantonen dat aan de voorgestelde Epv is voldaan. Op de infrastructuur voor de elektronische gegevensuitwisseling en voor de gegevensuitwisseling zelf, zullen PIA's moeten worden uitgevoerd. Het is voorstelbaar dat GuStan daarnaast een model PIA ontwikkelt voor zorgaanbieders, zorginstellingen en zorgverzekeraars.

2.1.8 Functionaris Gegevensbescherming (FG)

Gezien de criteria die van toepassing zijn om te bepalen of een FG verplicht moet worden aangesteld, zullen vele ondernemingen die actief zijn binnen de langdurige zorg een FG moeten aanstellen.
In de concept Algemene Maatregel van Bestuur (AMvB) 'Besluit houdende nadere regels over functionele, technische en organisatorische gegevensverwerking door en tussen zorgaanbieders

(elektronische gegevensuitwisseling tussen zorgaanbieders)' is ook de verplichting opgenomen dat de verantwoordelijke voor een elektronisch uitwisselingssysteem een FG benoemt.[28]

2.1.9 Privacybeleid

Binnen het project GuStan zal beleid moeten worden opgesteld hoe om te gaan met de privacyaspecten binnen de verschillende deelprojecten en aan welke eisen de resultaten moeten voldoen. Dit kan een afgeleide zijn van het privacybeleid van het ministerie VWS. Voorwaarde is wel dat dit beleid reeds rekening houdt met de eisen vanuit de voorgestelde Europese privacyverordening.

Het is aan te bevelen in het privacybeleid aandacht te besteden aan de bewaartermijn van gegevens die met elektronische uitwisselingssystemen worden verwerkt, alsook aan de bewaartermijn van logging-gegevens.[29] Tevens is het goed aandacht te besteden aan de logging van het uitwisselingssysteem zelf, en de normen waaraan deze moet voldoen. Ook is het aan te bevelen om aandacht te besteden aan gegevensbeveiliging en de normen waaraan deze moet voldoen; aan het voldoen aan het toestemmingsvereiste en de aanwijzing van een FG.

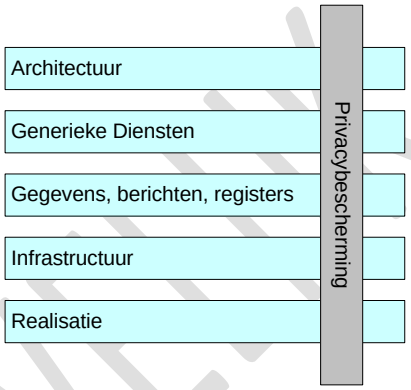
Speciale aandacht zal hierin moeten worden besteed aan de gegevensuitwisseling met organisaties in andere landen. In de Epv zijn namelijk restricties opgenomen ten aanzien van de gegevensuitwisseling met landen buiten de Europese Unie (een derde land) of naar een internationale organisatie. Pas als is vastgesteld dat een passend beschermingsniveau wordt gewaarborgd is de uitwisseling onder bepaalde voorwaarden mogelijk. Inbouw van een raamwerk dat inzicht geeft in de verbanden van "Legal entities" kan een belangrijke bijdrage leveren bij het identificeren van de landen waarin de betrokken organisaties zijn gevestigd.

[28] *Kamerstukken II*, 33509, bijlage bij nr. 7.

[29] In overleg met het CBP stellen vertegenwoordigende organisaties van zorgaanbieders en patiënten een bewaartermijn vast voor logging.

3 Aanpak

Het realiseren van de privacybescherming binnen het project GuStan gaat over alle deelprojecten heen. Dit betekent dat elk deelproject er voor moet zorgen dat die aspecten van de privacybescherming die een rol spelen binnen het betreffende deelproject moeten worden geadresseerd. Zo zullen bijvoorbeeld in het deelproject Infrastructuur technische en organisatorische maatregelen moeten worden genomen om het vereiste (hoge) niveau van beveiliging te waarborgen.



Daarentegen zijn er ook activiteiten die GuStan-breed kunnen worden gerealiseerd, en misschien zelfs op een later moment wel VWS breed kunnen worden toegepast. Hierbij moet worden opgemerkt dat niet alle in de voorgaande hoofdstukken beschreven onderwerpen 1-op-1 geadresseerd moeten worden. Bijvoorbeeld voor het onderwerp 'Profiling' kan worden volstaan met een nadere uitwerking in het Privacybeleid. Hetzelfde geldt voor de functionaris gegevensbescherming (FG).

3.1 Activiteiten

De volgende activiteiten met betrekking tot de privacybescherming zullen moeten worden opgepakt. De GuStan-brede resultaten zijn daarna beschikbaar voor de verschillende deelprojecten en ook voor de partijen die betrokken zijn bij de gegevensuitwisseling.

3.1.1 Uitvoeren generieke PIA met betrekking tot de gegevensuitwisseling in de langdurige zorg

Een PIA is bij uitstek geschikt als startpunt voor het opstellen van het privacybeleid en de invulling van de privacybescherming. De (privacy)risico's worden in kaart gebracht en het rapport geeft aanbevelingen op welke wijze deze risico's kunnen worden gemitigeerd.

3.1.2 Het opstellen van het Privacybeleid gegevensuitwisseling in de langdurige zorg

Het privacybeleid met betrekking tot de gegevensuitwisseling in de langdurige zorg moet de richtlijnen bevatten voor de wijze waarop de privacybescherming met betrekking tot de gegevensuitwisseling vorm wordt gegeven. Hierin zullen alle in de voorgaande hoofdstukken beschreven onderwerpen moeten worden geadresseerd.

De basis voor het privacybeleid Gegevensuitwisseling zou het huidige informatiebeveiligings- en privacybeleid van het ministerie VWS kunnen zijn. Dit zal in ieder geval moeten worden aangescherpt op twee aspecten:

1. De voorgestelde Europese privacyverordening en andere ontwikkelingen zoals de meldplicht datalekken. Dit natuurlijk tot zover deze actualisering van het beleid al niet onderhanden is.
2. De specifieke NEN-normen.
3. De specifieke hiervoor benoemde aandachtsgebieden voor de gegevensuitwisseling, zoals de mogelijkheden van het verlenen van generieke en beperkte toestemming.

Hierbij zal rekening moeten worden gehouden met de algemene wetgeving zoals de Wbp en de aanstaande Epv, alsmede met de specifieke wetgeving binnen de zorg zoals bijvoorbeeld de Wet gebruik burgerservicenummer in de zorg (of na doorvoering van de betreffende wetswijziging de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg).

Ook zal in het Privacybeleid rekening moeten worden gehouden met de eisen die worden gesteld aan de diverse ‘producten’ van GuStan, denk bijvoorbeeld aan de Generieke Diensten. Het ligt voor de hand dat er vanuit privacyperspectief eisen zullen worden gesteld aan deze Generieke Diensten. Maar bijvoorbeeld ook aan de infrastructuur of de inrichting en het gebruik van de taxonomie.

Het privacybeleid (of een gedeelte daarvan) moet ook beschikbaar komen voor de partijen die betrokken zijn bij de gegevensuitwisseling zodat deze partijen kennis kunnen nemen zodat ook zij aan de eisen kunnen (gaan) voldoen.

3.1.3 De inrichting van de informatieplicht

In het privacybeleid worden (vanzelfsprekend) de kaders voor de informatieplicht opgenomen. Belangrijk aspect hierbij is wie is verantwoordelijk voor de inrichting en uitvoering van de informatieplicht. Er zullen partijen moeten worden aangewezen die invulling moeten geven aan de informatieplicht. Dit kan bijvoorbeeld de verzender van de gegevens zijn.

Het lijkt voor de hand te liggen dat er door GuStan in ieder geval invulling wordt gegeven aan de inrichting van de informatieplicht over de algemene aspecten van de gegevensuitwisseling binnen de langdurige zorg. Dit moet aansluiten op de informatieplicht die is/wordt belegd bij de verantwoordelijke partij(en).

3.1.4 Inrichting meldplicht datalekken

Hetgeen in de vorige paragraaf (§ 4.1.3) is beschreven ten aanzien van de informatieplicht geldt ook voor de inrichting van de meldplicht datalekken.

3.1.5 Inrichting van de rechten van betrokkenen

Hetgeen in paragraaf § 4.1.3 is beschreven ten aanzien van de informatieplicht geldt min of meer ook voor de inrichting van de rechten van betrokkenen.
Ten aanzien van de onderwerpen recht op toegang tot zijn gegevens, recht op rectificatie, recht om vergeten te worden, recht om gegevens te laten wissen en recht van bezwaar geldt natuurlijk dat deze ook van toepassing zijn voor gegevensuitwisseling. De gegevensuitwisseling zal er in moeten voorzien dat als een cliënt een van zijn of haar rechten inroept dit ook zijn effect kan hebben voor de ontvangers van de gegevens.

Het recht van gegevensoverdraagbaarheid en gegevensuitwisseling heeft ook een directe relatie. De voorzieningen voor de gegevensuitwisseling tussen partijen kan ook worden toegepast voor de uitwisseling van gegevens op verzoek van de betrokkene. De gegevensoverdraagbaarheid kan worden aangeboden als een Generieke Dienst. Ook zou er een Generieke Dienst kunnen worden ontwikkeld voor het gegeven van toestemming voor overdracht van gegevens, in lijn met de hiervoor genoemde bepalingen in de aankomende Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg.

3.1.6 Inrichting PbD*2

Als uitwerking van het (privacy)beleid in zake PbD*2 zullen mogelijk een aantal concrete uitwerkingen van het beleid vorm moeten worden gegeven. Denk hierbij bijvoorbeeld aan de wijze waarop invulling wordt gegeven aan het de-personaliseren van de gegevens voor statistische of andere doeleinden. Een ander onderwerp dat zeker een belangrijke rol speelt bij gegevensuitwisseling, is de wijze waarop invulling wordt gegeven aan de sticky policies. Bij de inrichting van PbD*2 zullen deze onderwerpen zeker moeten worden geadresseerd.
Welke andere concrete producten door GuStan moeten worden opgeleverd kan worden bepaald op het moment dat dit onderwerp nader is uitgewerkt in het Privacybeleid. De producten kunnen zelf worden ontwikkeld, worden aangeschaft, worden hergebruikt vanuit het ministerie VWS of van andere overheidsinstellingen.

Doelstelling is dat de producten zowel toegepast kunnen worden binnen de deelprojecten van GuStan als door de andere partijen die betrokken zijn bij de gegevensuitwisseling in de langdurige zorg.