MedMij

Te onderscheiden rollen in het afsprakenstelsel

DIGITAL ME

Eindhovenseweg 22a | 5281 RA Boxtel | NL | +31 (0)411 61 65 65 | info@digital-me.nl | digital-me.nl
IBAN: NL88 RABO 0129 8756 51 | BIC: RABONL2U | KvK: 17 20 09 66 | VAT: NL 8181 68 183 B01

Inhoudsopgave

1 Context

MedMij stelt spelregels op voor het uitwisselen en gebruiken van gezondheidsgegevens. Producten en organisaties die het MedMij-logo tonen, moeten zich aan deze spelregels houden. Het betekent dat zij op een door Medmij goedgekeurde manier gegevens met elkaar uitwisselen en veilig en betrouwbaar met deze gegevens omgaan.

Een persoonlijke gezondheidsomgeving (PGO) is een digitale omgeving (bestaande uit apps, devices en verbindingen) die je in staat stelt om al je relevante gezondheidsgegevens, die verspreid staan opgeslagen bij zorgaanbieders en overheden, overzichtelijk en veilig in te zien, aan te vullen met eigen metingen en te delen met wie je dat wilt.[1]

Een PGO met het MedMij-logo moet voldoen aan de standaarden en basiseisen van Medmij. Met de verbindingen op de gegevens van zorgaanbieders gefaciliteerd door Medmij in combinatie met een zelf gekozen en ingerichte PGO kan straks iedereen die dat wil betrouwbaar over zijn of haar eigen gezondheidsinformatie beschikken en deze desgewenst naar eigen inzicht delen.[2] Zo wordt het mogelijk voor een individu om via Medmij toegang te krijgen tot zijn of haar medische gegevens en om deze zelf naar eigen goeddunken te verwerken in een PGO. Daarbij krijgt de individu niet alleen de beschikking over gegevens afkomstig van zorgaanbieders, maar ook over gegevens van hemzelf en bijvoorbeeld van apps die gezondheidsaspecten meten en/of sportprestaties meten en bijhouden.

1.1 Ambitie

De ambitie is er op gericht individuen die dat willen, in staat te stellen om hun PGO's te verbinden met andere informatiesystemen (inclusief de informatiesystemen van beheerders van Elektronische Patiënten Dossiers), waardoor zij in staat worden gesteld een persoonlijk zorgnetwerk te creëren van zorgaanbieders en om de regie te voeren over de zorgprocessen in dat persoonlijke zorgnetwerk:

> "De patiënt heeft volledige zeggenschap over zijn PGD[3]. Hij bepaalt wat er wel en niet in staat of wat wel en niet zichtbaar is voor anderen. Ook kan de patiënt kiezen wie hij bepaalde rechten geeft ten aanzien van zijn PGD. De patiënt kan zelf beschikken over de informatie in het PGD en die delen met diegenen die hij zelf kiest."[4]

---

1 Zie: http://www.medmij.nl/wat-is-medmij/.

2 Zie: http://www.medmij.nl/wat-is-medmij/.

3 PGD = PGO. Zie: https://www.patientenfederatie.nl/themas/persoonlijke-gezondheidsomgeving/.

4 Bierma, L. & M. Heldoorn "Het persoonlijk gezondheidsdossier. De visie van patiëntenfederatie NPCF", Patiëntenfederatie NPCF, 2e druk, juni 2013: p.21.

1.2 Kenmerken PGO

Een persoon die een PGO beheert kan:

- zorgaanbieders toestemming verlenen om gegevens toe te voegen aan zijn of haar PGO;
- zorgaanbieders toestemming verlenen om gegevens uit zijn of haar PGO te gebruiken voor communicatie tussen zorgaanbieders.
- het gradatieniveau aanpassen, waarop gegevens worden uitgewisseld en aan wie gegevens kunnen worden uitgewisseld (naam zorgaanbieder, soort zorgaanbieder, naam zorginstelling of soort zorginstelling);
- beslissen welke gegevens worden uitgewisseld;
- beslissen voor hoe lang zorgaanbieders de gegevens mogen inzien;
- toestemming verlenen voor (anoniem!) gebruik van (een deel van) de PGO-gegevens in wetenschappelijke en andere studies.[5]

De Patëntenfederatie NPCF wenst[6], en de Europese algemene verordening gegevensbescherming (AVG)[7] vereist, gegevensbescherming door ontwerp ('Data Protection by Design') en gegevensbescherming door standaardinstellingen ('Data Protection by Default').[8/9] Ook worden strenge eisen gesteld aan beveiliging[10] en aan het

---

5 Bierma, L. & M. Heldoorn "Het persoonlijk gezondheidsdossier. De visie van Patiëntenfederatie NPCF", Patiëntenfederatie NPCF, 2e druk, juni 2013: 22. Hierin wordt overigens gesproken over 'zorgverleners'. Dit begrip wordt in de (onlangs aangepaste) Wet gebruik burgerservicenummer in de zorg gedefinieerd als: "natuurlijke persoon die in een register als bedoeld in artikel 3 van de Wet op de beroepen in de individuele gezondheidszorg staat ingeschreven of die een beroep uitoefent waarvan de opleiding krachtens artikel 34, eerste lid, van die wet is geregeld of aangewezen". Wij geven de voorkeur aan het gebruik van het bredere begrip 'zorgaanbieder' (hieronder vallen bijvoorbeeld ook mantelzorgers en andere hulpverleners).

6 Bierma, L. & M. Heldoorn "Het persoonlijk gezondheidsdossier. De visie van patiëntenfederatie NPCF", Patiëntenfederatie NPCF, 2e druk, juni 2013: 21-22.

7 Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming), *PbEU* 4 mei 2016, L119: 1-88.

8 'Gegevensbescherming door ontwerp' en 'Gegevensbescherming door standaardinstellingen' zijn algemene beginselen inzake de verwerking van persoonsgegevens. Zie Overwegingen 78 en 108 Preambule AVG en art. 25 AVG.

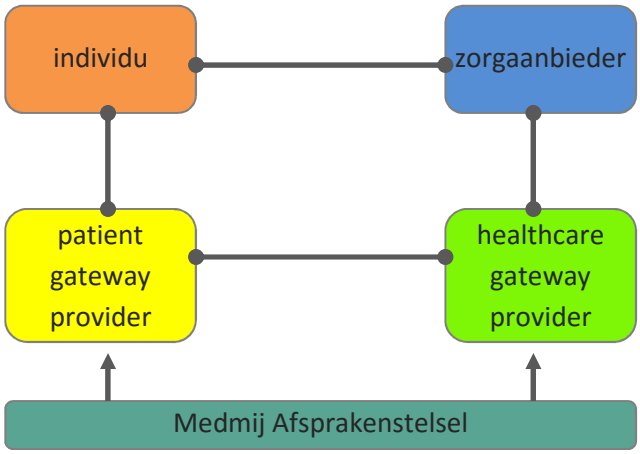
9 Overweging 53 Preambule AVG: "Om de naleving van deze richtlijn te kunnen aantonen, dient de verwerkingsverantwoordelijke intern beleid vast te stellen en maatregelen te implementeren die in het bijzonder voldoen aan de beginselen van gegevensbescherming door ontwerp en gegevensbescherming door standaardinstellingen."

10 Art. 32 AVG.

voorkomen van inbreuk in verband met persoonsgegevens[11], met meldplichten voor het geval zich toch een inbreuk zou voordoen.[12]

2 Te onderscheiden *functionele* rollen binnen het MedMij afsprakenstelsel

Binnen het MedMij afsprakenstelsel dienen vier rollen te worden onderscheiden **('4-corner' model** van gegevensuitwisseling).



Aan de ene kant is dat de individu als gebruiker van een of meerdere PGO's en zijn of haar 'gateway provider' en aan de andere kant de zorgaanbieder met een 'gateway provider'. 'Gateway providers' zijn beheerders van systemen die kunnen zorgen voor de (technische) uitwisseling van gegevens tussen PGO beheerders en zorgaanbieders.

In het beoogde MedMij afsprakenstelsel worden twee soorten 'Gateways' onderscheiden: 'Patient Gateway' en 'Healthcare Gateway'.

De rol van '**Patient Gateway provider'** is bedoeld om ervoor te zorgen dat persoonsgegevens vanuit een PGO op een betrouwbare manier en op basis van de eisen die hieraan worden gesteld, worden opgehaald bij, of ter beschikking gesteld worden aan zorgaanbieders via de 'Healthcare Gateway provider'.

De rol van **'Healthcare Gateway provider'** is bedoeld om de informatiesystemen van zorgaanbieders te koppelen aan PGO's van individuen via de 'Patient Gateway provider'.

---

[11] 'inbreuk in verband met persoonsgegevens' wordt omschreven als "een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens". Dit Europese begrip lijkt derhalve breder te zijn dan het begrip 'datalek' dat in de Wet bescherming persoonsgegevens wordt gehanteerd.

[12] Artt. 33 en 34 AVG.

Al deze partijen spelen een rol bij de verwerking van persoonsgegevens. Afhankelijk van de rol die zij hierbij vervullen, vallen zij wel of niet onder de AVG of onder andere relevante regelgeving. Bovendien kan elk van deze partijen, bij de vervulling van haar rol, voor de dienstverlening een externe derde inschakelen. Het is dan ook noodzakelijk om goed in kaart te brengen hoe precies de logische en de fysieke informatiestromen (zullen) lopen binnen het MedMij afsprakenstelsel. Aan de hand daarvan kunnen, naast de functionele rollen, dan ook de juridische rollen van de betrokken partijen worden bepaald. Afhankelijk van de juridische rol van een partij is bepaalde regelgeving wel of niet van toepassing. Het is van groot belang dit goed te analyseren, omdat verschillende juridische rollen door de Europese wetgever zijn gekoppeld aan verschillende niveaus van aansprakelijkheid.

3 Te onderscheiden *juridische* rollen binnen het MedMij afsprakenstelsel

De AVG is van toepassing op **verwerkingsverantwoordelijken** en op **verwerkers**.
De AVG omschrijft 'verwerkingsverantwoordelijke' als "een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt"[13], en 'verwerker' als "een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt".[14]

De AVG is niet van toepassing op gebruikers van een PGO, zolang dat **natuurlijke personen** zijn die een zuiver persoonlijke of huishoudelijke activiteit uitoefenen.[15] In veel gevallen zal het echter zo zijn dat de PGO van een individu wordt gehost door een andere partij: een '**hosting provider**'.[16] 'Hosting providers' zouden daardoor onder de definitie van 'verwerker' in de zin van de AVG kunnen komen te vallen, waardoor zij zich aan de regels van de AVG die gelden voor verwerkers zullen moeten houden en waardoor ook de aansprakelijkheden (en boetes bij overtredingen) die gelden voor verwerkers op hen van toepassing zullen zijn. Veel 'hosting providers' zullen daar niet op zitten te wachten.

---

13 Art. 4 onder 7) AVG.

14 Art. 4 onder 8) AVG.

15 Art. 2, lid 2 onder c) AVG.

16 Art. 14. Lid 1, Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt ("Richtlijn inzake elektronische handel"), *PbEG* nr. L 178 van 17/07/2000: 1-16 omschrijft "Hosting" ("host"-diensten) als "een dienst van de informatiemaatschappij [die] bestaat in de opslag van de door een afnemer van de dienst verstrekte informatie."

De AVG kent echter een bepaling waarin staat:

> "Deze verordening laat de toepassing van Richtlijn 2000/31/EG, en met name van de regels in de artikelen 12 tot en met 15 van die richtlijn betreffende de aansprakelijkheid van als tussenpersoon optredende dienstverleners onverlet."[17]

Het betreft hier een aantal bijzondere aansprakelijkheidsbepalingen in de richtlijn inzake 'Elektronische handel'[18] die gelden voor de aansprakelijkheid van dienstverleners die als tussenpersoon optreden[19], zoals bijvoorbeeld 'hosting providers'. Deze bijzondere aansprakelijkheidsbepalingen zijn door de Nederlandse wetgever overgenomen in het Burgerlijk Wetboek. Op grond hiervan moet worden geconcludeerd dat wanneer een dienst van de 'hosting provider' bestaat in de opslag van de door een afnemer van de dienst verstrekte informatie, de 'hosting provider' niet aansprakelijk is voor de op verzoek van de afnemer van de dienst opgeslagen informatie, op voorwaarde dat:

- de 'hosting provider' niet daadwerkelijk kennis heeft van een eventuele onwettige activiteit of informatie en, wanneer het een schadevergoedingsvordering betreft, geen kennis heeft van feiten of omstandigheden waaruit het onwettige karakter van de activiteiten of informatie duidelijk blijkt; of,
- de 'hosting provider', zodra hij van het bovenbedoelde daadwerkelijk kennis heeft of besef krijgt, prompt handelt om de informatie te verwijderen of de toegang daartoe onmogelijk te maken.

Een 'hosting provider' die met een klant een 'data hosting' overeenkomst sluit zal zich in ieder geval kunnen beroepen op de bijzondere regeling van aansprakelijkheid in de regeling van de richtlijn inzake 'Elektronische handel'.

Het bovenstaande geldt uiteraard niet alleen voor een 'hosting provider' die een gegevensopslagdienst aanbiedt aan een natuurlijk persoon; het geldt in dezelfde mate voor een 'hosting provider' die een gegevensopslagdienst aanbiedt voor een zorgaanbieder.

Let wel:
de hierboven beschreven bijzondere aansprakelijkheidsregeling voor 'hosting providers' geldt alleen,

---

17 Art. 2, lid 4 AVG.

18 Art. 14 Richtlijn inzake elektronische handel.

19 Overweging 21 Preambule AVG.

> "voor gevallen waarin de activiteit van de aanbieder van diensten van de informatiemaatschappij beperkt is tot het technische proces van werking en het verschaffen van toegang tot een communicatienetwerk waarop door derden verstrekte informatie wordt doorgegeven of tijdelijk wordt opgeslagen, met als enig doel de doorgifte efficiënter te maken. Die activiteit heeft een louter technisch, automatisch en passief karakter, hetgeen inhoudt dat de aanbieder van diensten van de informatiemaatschappij noch kennis noch controle heeft over de informatie die wordt doorgegeven of opgeslagen". [20]

Een 'hosting provider' die ten behoeve van een individu een PGO inricht (of de informatie daarin zelfs verrijkt) doet duidelijk meer dan uitsluitend het (technische) opslaan van gegevens en zal daarom al snel ook als verwerker of zelfs als verwerkingsverantwoordelijke in de zin van de AVG aangemerkt kunnen worden. Dit is ook het geval wanneer een zorgaanbieder gebruik maakt van een platform voor het opslaan van persoonsgegevens en de beheerder van dat platform aanvullende diensten levert (zoals bijv. verrijking of analyse van de opgeslagen persoonsgegevens).

Een persoon, een PGO gebruiker, kan besluiten persoonsgegevens vanuit zijn of haar PGO te routeren naar personen of organisaties die daarom vragen (zoals een zorgaanbieder). Dit gebeurt in het MedMij afsprakenstelsel onder gebruikmaking van de diensten van de hierboven in paragraaf 4 beschreven 'Gateway providers'.

Nu zijn er Europese regels die van toepassing zijn "op de verwerking van persoonsgegevens in verband met de levering van openbare elektronische communicatiediensten over openbare communicatienetwerken in de Gemeenschap, met inbegrip van openbare communicatienetwerken die systemen voor gegevensverzameling en identificatie ondersteunen." Deze regels zijn vervat in de richtlijn betreffende privacy en elektronische communicatie.[21]

'Gateway providers' kunnen worden gezien als **aanbieders van openbare elektronische communicatiediensten** in de zin van de Europese richtlijn betreffende privacy en

---

[20] Overweging 42, Preambule Richtlijn inzake elektronische handel.

[21] Art. 3, Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), *PbEU* 31/07/2002 nr. L 201: 37-47 zoals gewijzigd in art. 2 onder 3) van Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronische communicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming, *PbEU* 18.12.2009, nr. L 337: 11-36 op p. 29.

elektronische communicatie. De bepalingen van deze richtlijn zijn door de Nederlandse wetgever opgenomen in de Telecommunicatiewet.

Een 'elektronische communicatiedienst' is, in het kader van bovengenoemde richtlijn:

> "een gewoonlijk tegen vergoeding aangeboden dienst die geheel of hoofdzakelijk bestaat in het overbrengen van signalen via elektronische-communicatienetwerken, waaronder telecommunicatiediensten en transmissiediensten op netwerken die voor omroep worden gebruikt, doch niet de dienst waarbij met behulp van elektronische-communicatienetwerken en -diensten overgebrachte inhoud wordt geleverd of redactioneel wordt gecontroleerd. Hij omvat niet de diensten van de informatiemaatschappij zoals omschreven in artikel 1 van Richtlijn 98/34/EG, die niet geheel of hoofdzakelijk bestaan uit het overbrengen van signalen via elektronische-communicatienetwerken".

De richtlijn betreffende privacy en elektronische communicatie schrijft voor dat de aanbieder van een openbare elektronische communicatiedienst passende technische en organisatorische maatregelen dient te treffen "om de veiligheid van zijn diensten te garanderen, indien nodig in overleg met de aanbieder van het openbare communicatienetwerk wat de veiligheid van het netwerk betreft. Die maatregelen waarborgen een beveiligingsniveau dat in verhouding staat tot het betrokken risico, rekening houdend met de stand van de techniek en de kosten van uitvoering ervan." Deze eis is in deze richtlijn niet specifiek gerelateerd aan de verwerking van persoonsgegevens, maar geldt in algemene zin.

Deze richtlijn is derhalve van toepassing op partijen in het afsprakenstelsel die data distribueren, transporteren en/of routeren; deze vervullen de rol van aanbieder van een openbare elektronische communicatiedienst, maar zij kunnen in veel gevallen niet per se ook worden aangemerkt als verwerkingsverantwoordelijke of verwerker van persoonsgegevens in de zin van de AVG. Vaak zullen zij niet eens weten waarop de data die zij distribueren, transporteren en/of routeren betrekking hebben; dit omdat die data conform het beveiligingsbeleid meestal versleuteld zullen zijn en zij geen toegang hebben tot de bijbehorende sleutels.

Voor partijen in het afsprakenstelsel die een rol vervullen waarop de richtlijn betreffende privacy en elektronische communicatie van toepassing is geldt dat zij passende technische en organisatorische maatregelen dienen te treffen om de veiligheid van hun diensten te garanderen, "indien nodig in overleg met de aanbieder van het openbare communicatienetwerk wat de veiligheid van het netwerk betreft. Die maatregelen waarborgen een beveiligingsniveau dat in verhouding staat tot het

betrokken risico, rekening houdend met de stand van de techniek en de kosten van uitvoering ervan."[22]

De maatregelen moeten ervoor zorgen dat in ieder geval, dat[23]:

- wordt gewaarborgd dat alleen gemachtigd personeel voor wettelijk toegestane doeleinden toegang heeft tot de persoonsgegevens;
- opgeslagen of verzonden persoonsgegevens worden beschermd tegen onbedoelde of onwettige vernietiging, onbedoeld verlies of wijziging, en niet-toegestane of onwettige opslag, verwerking, toegang of vrijgave; en,
- een beveiligingsbeleid wordt ingevoerd met betrekking tot de verwerking van persoonsgegevens.

Op grond van deze richtlijn hebben aanbieders van een openbare elektronische communicatiedienst een meldplicht in geval van een inbreuk in verband met persoonsgegevens.[24] Zoals hierboven reeds aangegeven is het echter nog maar de vraag of zij überhaupt weten dat er persoonsgegevens worden verwerkt in de datastromen die zij managen. Dit hangt samen met de vraag of het verkeer is versleuteld en wie er toegang heeft tot de sleutels.

In ieder geval kent deze richtlijn eigen regels waar het gaat om de verwerking van persoonsgegevens door een aanbieder van een openbare elektronische communicatiedienst, waar het gaat om inbreuken in verband met persoonsgegevens en waar het gaat om inbreuken in verband met persoonsgegevens. Dit lijkt onnodig en is nodeloos verwarrend. De AVG zegt hierover het volgende[25]:

> "Deze verordening dient van toepassing te zijn op alle aangelegenheden die betrekking hebben op de bescherming van grondrechten en fundamentele vrijheden in het kader van de verwerking van persoonsgegevens waarvoor de in Richtlijn 2002/58/EG van het Europees Parlement en de Raad opgenomen specifieke verplichtingen met dezelfde doelstelling niet gelden, met inbegrip van de verplichtingen van de verwerkingsverantwoordelijke en de rechten van natuurlijke personen. Om de verhouding tussen deze verordening en Richtlijn 2002/58/EG te verduidelijken, dient die richtlijn dienovereenkomstig te worden gewijzigd. Zodra deze verordening is vastgesteld, dient Richtlijn 2002/58/EG te worden geëvalueerd, met name om te zorgen voor samenhang met deze verordening".

---

[22] Art. 4 richtlijn betreffende privacy en elektronische communicatie.

[23] Art. 1*bis* richtlijn betreffende privacy en elektronische communicatie.

[24] Art. 4, lid 3 richtlijn betreffende privacy en elektronische communicatie.

[25] Overweging 173 Preambule AVG.

4 Conclusies

Op grond van bovenstaande uiteenzetting moet geconcludeerd worden dat vanuit het oogpunt van de relevante wetgeving, de volgende rollen onderscheiden dienen te worden in het kader van het MedMij afsprakenstelsel, naast de functionele rollen van individu, zorgaanbieder, 'Patient Gateway provider' en 'Healthcare Gateway provider', de volgende juridisch relevante rollen onderscheiden dienen te worden:

- Verwerkingsverantwoordelijke
- Verwerker
- Hosting Provider
- Aanbieder PGO
- Aanbieder van een openbare elektronische communicatiedienst

Afhankelijk van de (juridische) rol die een betrokken partij in het MedMij afsprakenstelsel vervult is een andersoortige set van verplichtingen, verantwoordelijkheden en aansprakelijkheden van toepassing.

Het is dan ook zaak om vast te stellen welke partijen ten aanzien van elke functie die in het document 'Basisdefinitie afsprakenstelsel MedMij' is benoemd, een rol spelen, om vervolgens te analyseren welke juridische rol dit dan is. Op grond daarvan kan dan weer worden beoordeeld welke set van regels op de desbetreffende partij van toepassing is.

Boxtel, 10 november 2016