**Privacybeleid**

**Classificatie: Openbaar**

Privacy gaat over persoonsgegevens en dienen beschermd te worden conform huidige wet – en regelgeving. Bescherming van de privacy regelt onder andere onder welke voorwaarden persoonsgegevens gebruikt mogen worden. Persoonsgegevens zijn hierbij alle gegevens die herleidbaar zijn tot een bepaald individu

De Raad van Bestuur heeft ter bescherming van de persoonlijke levenssfeer van cliënten een Beleid opgesteld houdende de regels voor de registratie van persoonsgegevens en de verwerking daarvan en is zo opgesteld dat het aan de vereisten van de wet- en regelgeving voldoet, in onder andere:

- Algemene Verordening Gegevensbescherming (AVG)
- Uitvoeringswet AVG (UWAVG)
- Europees Verdrag voor de Rechten van de Mens
- Archiefwet
- Auteurswet
- Telecommunicatiewet (inclusief de bijbehorende besluiten)
- Burgerlijk Wetboek (BW)
- Wet Maatschappelijke Ondersteuning (WMO)
- Wet langdurige zorg (Wlz)
- Wet Langdurige Zorg (WLZ)
- Zorgverzekeringswet (ZVW)
- Wet Zorg en Dwang (WZD)
- Wet op de Geneeskundige Behandelingsovereenkomst (WGBO)
- Wet Kwaliteit, klachten en geschillen zorg(Wkkgz)
- Wet elektronische verwerking van gegevens (Wevg)
- De Wet beveiliging netwerk- en informatiesystemen (Wbni)
- Wet Algemeen Gegevensbeheer Zorgverleners. (AGB
- Europese Network and Information Systems-richtlijn (NIS2

**Doel**
Gebruikers te informeren over welke informatie van hen wordt verzameld en hoe deze zal worden gebruikt.

Beleidsregels te stellen aan medewerkers voor het verwerken van persoonsgegevens, zodat de privacy van cliënten gegarandeerd is en beveiligings- en privacy-incidenten en de eventuele gevolgen hiervan worden voorkomen.

Bij te dragen aan de transparantie van de regels die door de organisatie worden gehanteerd met betrekking tot de verwerking van persoonsgegevens.

Een uitvoerend kader te scheppen om de naleving van de verantwoordingsplicht zoals gesteld in art. 5 AVG na te komen.

**Reikwijdte**
Dit Beleid is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens en de verwerking van persoonsgegevens die in een bestand zullen worden opgenomen betreffende cliënten die zorg van de organisatie (wensen te) ontvangen of zorg hebben ontvangen.
Privacy aspecten met betrekking tot de medewerkers worden opgenomen in het **Privacy HR-beleid**.

**Uitgangspunten**

Binnen de organisatie is het veilig en betrouwbaar omgaan met informatie de verantwoordelijkheid van iedereen. Hierbij hoort het actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen informatie en van de fysieke documenten.

De organisatie sluit met alle leveranciers **verwerkersovereenkomsten** af als zij persoonsgegevens verwerken van de organisatie.

Regelmatig (minimaal jaarlijks) wordt geëvalueerd en wordt gekeken of aanpassing van beleid, procedures en richtlijnen gewenst is.

**Verwerking van Persoonsgegevens**
De verwerking van persoonsgegevens is gebaseerd op één van de **wettelijke grondslagen.**

**De zes grondslagen zijn:**

1. **Toestemming** van betrokkene
2. **Uitvoering van een overeenkomst** waarbij de betrokkene partij is
3. Nakoming van een **wettelijke verplichting** waaraan de organisatie onderworpen is
4. Vrijwaring van een **vitaal belang** van betrokkene;
5. Vervulling van een **taak van algemeen belang** (overheid)
6. De behartiging van het **gerechtvaardigde** belang van de organisatie die persoonsgegevens verwerkt, tenzij het belang of de grondrechten en de fundamentele vrijheden van de betrokkene zwaarder wegen.

**De grondslagen voor de organisatie zijn**

- Noodzakelijk is voor de **uitvoering van een overeenkomst** waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van een betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst
- Noodzakelijk is om een **wettelijke verplichting** na te komen
- Noodzakelijk is voor de behartiging van het **gerechtvaardigde belang** van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang van de betrokkene zwaarder weegt dan van de verantwoordelijke.
- De cliënt hiertoe ondubbelzinnig zijn **toestemming** heeft verleend

**Verwerken van persoonsgegevens**
Onder verwerking wordt verstaan elke handeling met betrekking tot persoonsgegevens.
De wet noemt als voorbeelden van verwerking:

- Het verzamelen
- Opvragen
- Raadplegen
- Gebruiken
- Bijwerken
- Wijzigen
- Ordenen
- Vastleggen
- Bewaren
- Samenbrengen, met elkaar in verband brengen
- Verstrekking door middel van doorzending
- Verspreiding of enige andere vorm van terbeschikkingstelling
- Afschermen, uitwissen en vernietigen van gegevens.

**De persoonsgegevens worden op een behoorlijke en zorgvuldige wijze verwerkt zoals:**

- Het doel van de Verwerking moet voorafgaande aan de Verwerking voldoende specifiek en helder omschreven zijn. ‘
- Een verwerking van persoonsgegevens is gebaseerd op één van de wettelijke grondlagen zoals genoemd in artikel 6 van de AVG
- Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.
- Er worden niet meer gegevens verzameld dan noodzakelijk is voor het doel dat men wil bereiken. Gegevens dienen toereikend, ter zake dienend en niet bovenmatig te zijn.
- Verwerking van persoonsgegevens gebeurt op de minst ingrijpende wijze en dient in redelijke verhouding te staan tot het beoogde doeleinde (subsidiariteits- en proportionaliteitsbeginsel).
- Er worden maatregelen getroffen om zoveel mogelijk te waarborgen dat de te verwerken Persoonsgegevens juist en actueel zijn
- Voor betrokkenen is het inzichtelijk in hoeverre en op welke manier er persoonsgegevens worden verwerkt. Informatie en communicatie hierover moet eenvoudig toegankelijk en begrijpelijk zijn.

**Welke persoonsgegevens cliënten verwerkt de organisatie**
**Categorie**

- Algemene persoonsgegevens
- Bijzondere persoonsgegevens
- Cookies

**Algemene Persoonsgegevens**

- Zoals naam, adres, BSN, geslacht, geboortedatum, contactgegevens
- Contactgegevens 1st contactpersoon client
- Wettelijk vertegenwoordiger ( indien van toepassing)
- Contactgegevens van zorgverleners (huisarts, Apotheek, Specialist, maatschappelijk werk e.d.) voor zover relevant voor het verrichten van de zorg/dienst verlening
- Verzekering en polisnummer
- Rekeningnummer (indien van toepassing)

**Bijzondere persoonsgegevens**

- Medische gegevens zoals diagnose, infectieziekte, overdrachten Huisarts en ziekenhuis
- Medicatie gegevens behandeling en medicatiegebruik (indien van toepassing)
- Incidentenregistratie
  Foto’s wond en incident, ter beoordeling van de voortgang (indien van toepassing)
- Gezondheid zoals gewicht en allergieën (indien van toepassing)
- Gegevens over de levensstijl, zoals rook- en drinkgewoonten
- Reanimatieverklaring (alleen op verzoek)
- Cameratoezicht in en rond de panden van MIJ

**Doel**

- Het opstellen en **uitvoeren van overeenkomsten**
- Het aanleggen en **bijhouden van een dossier** (ECD)
- Voor **communicatie** m.b.t de zorg/dienstverlening
- **Uitnodigen** voor een tevredenheidsonderzoek
- **Verificatie** ter controle juiste persoon.
- **Preventie toepassen** ter voorkoming van verspreiding
- **Calamiteiten**- en incidentenonderzoek.
- **Kwaliteitsbewaking** en kwaliteitsbevordering van de zorgverlening
- **Financiële afhandeling** van de geleverde zorg.
- Voor het maken van de **zorglegitimatie**
- Ten behoeve van de **veiligheid** en eigendommen van onze medewerkers cliënten en bezoekers

- **Het verbeteren** van de websitefunctionaliteit en gebruikerservaring. Raadpleeg ons Cookiebeleid op de website voor meer details.
- Het voldoen aan **wettelijke verplichtingen**

**Herkomst Persoonsgegevens:**

- De cliënt zelf
- Wettelijke vertegenwoordigers van de cliënt
- Huisarts, Ziekenhuis of andere Discipline
- Curatoren, bewindvoerders of mentoren van de cliënt
- Familieleden of anderen naasten van de cliënt, mits zij met goedkeuring van de cliënt handelen.

Indien persoonsgegevens worden verkregen van een Huisarts, Ziekenhuis, andere behandelaar of Discipline wordt aangenomen dat de client toestemming heeft gegeven voor de verstrekking, en op de hoogte is gebracht van doeleinde en waarvoor de verwerking gegevens bestemd zijn, door de verstrekker van de gegevens.

**Toegang tot de registratie van persoonsgegevens**

- Uitsluitend personen binnen de organisatie die daartoe zijn aangewezen door de verantwoordelijke en daartoe in het kader van hun taakuitoefening gerechtigd zijn, hebben toegang tot de verwerking van persoonsgegevens ( Autorisatie op basis van Need to Know)
- Een externe kan (beperkt) toegang worden verleend indien dit voor het uitvoer van zijn opdracht noodzakelijk is.
- Iedere gebruiker is van de persoonsgegevens is tot geheimhouding verplicht.

**Verstrekkingen van persoonsgegevens aan derden**

Wij sturen alleen gegevens van cliënten door aan derde partijen wanneer dit noodzakelijk is voor het uitvoeren van de zorgovereenkomst of wanneer wij hiertoe wettelijk verplicht zijn. Zo zijn wij als zorgorganisatie wettelijk verplicht om jaarlijks te kwaliteit van de zorg te meten. Om deze meting te kunnen laten uitvoeren verstrekken wij N.A.W gegevens aan het Meetbureau om u de vragenlijst te sturen. Voor cliënten is de deelname vrijwillig.

**Onder deze derden vallen onder andere** :

- CIZ
- Zorgkantoren voor het administratief afhandelen van de zorgtoewijzing
- Gemeentes in het kader van aanvragen van voorzieningen op het terrein van WMO, wonen en welzijn
- CAK voor het afhandelen van eigen bijdragen WLZ en WMO
- IGJ voor het beoordelen van rapport voorgekomen incidenten en calamiteiten.
- Betrouwbare derde partijen die ons ondersteunen bij het beheren van onze website en diensten.
- Meetbureau, voor tevredenheidsmetingen.

**In alle andere gevallen zoals het delen van persoonsgegevens met**

- Huisartsen
- Ziekenhuizen
- Andere behandelaren of disciplines is toestemming van de cliënt vereist.

Deze uitwisseling vindt plaats via beveiligde verbindingen, Zorgdomein en Point
Wanneer wij aan anderen gegevens verstrekken doen wij dit alleen nadat we uw toestemming hebben gekregen.
We verkopen of delen uw persoonlijke gegevens niet met derden voor marketingdoeleinden.

**Rechten van betrokkenen (cliënten)**
De AVG geeft betrokkenen diverse rechten.

**Recht op informatie**
De organisatie is wettelijk verplicht informatie te geven aan betrokkenen van wie zij persoonsgegevens verwerkt. Zij moet betrokkenen informeren welke persoonlijke gegevens zij verwerkt en met welk doel. De organisatie verleent deze informatie via het **privacy statement op de website** en ook via de privacyverklaring rechtstreeks aan de cliënt op het moment dat de persoonsgegevens worden verwerken.

**Recht op inzage**
Een cliënt kan bij een verzoek indienen om een overzicht van verwerkingen op te vragen o.a of de organisatie zijn persoonsgegevens gebruikt, en zo ja:

- om welke gegevens het gaat;
- wat het doel is van het gebruik alsmede de bewaartermijnen;
- aan wie de organisatie (*derden; buiten MOB*) de gegevens eventueel heeft verstrekt;
- wat de herkomst is van de gegevens.

**Recht op rectificatie**
Indien uit het verstrekte overzicht blijkt dat de persoonsgegevens feitelijk onjuist zijn, voor het doel van de verwerking onvolledig of niet ter zake dienend of in strijd zijn met een wettelijk voorschrift, kan de cliënt schriftelijk om verbetering, aanvulling, verwijdering en/of afscherming van het/de betreffende persoonsgegeven(s) verzoeken.

**Recht op beperking van de verwerking**
Indien de juistheid van persoonsgegevens door de cliënt worden betwist, de verwerking onrechtmatig is, de betrokkene de gegevens nodig heeft, of de cliënt bezwaar heeft gemaakt, dan kan een beroep worden gedaan op dit recht.

**Recht op overdraagbaarheid van gegevens**
Een cliënt heeft recht op overdraagbaarheid voor zover het gaat om door hem zelf verstrekte gegevens. Verzoeken worden intern behandeld en kunnen naar privacy@mij.nl worden gestuurd.

**Bewaring persoonsgegevens**
**Zorgdossier** De (persoons)gegevens van een cliënten in het zorgdossier vallen onder de WGBO worden gedurende 20 jaar bewaard of zoveel langer als redelijkerwijs nodig is te rekenen vanaf het tijdstip waarop client uit zorg gaan .

**Medicatie toedieningslijsten** dienen 2 jaar bewaard te worden. De cliënt is verplicht de papieren lijsten te bewaren. De organisatie is verantwoordelijk de lijsten te beheren.
Wanneer er op het gebied van medicatie een incident is voorgevallen waardoor de afgesproken toediening of aanreiking is verstoord dan dienen de toedieningslijsten 20 jaar te worden bewaard.
Wanneer er sprake is geweest van **volledig beheer over de medicatie** worden medicatiegegevens ook **20 jaar** bewaard.

**Ondersteuningsplannen WMO** geldt een bewaarplicht van 15 jaar

**Binnen één jaar na het verstrijken van de geldende bewaartermijn** worden de gegevens op een verantwoorde manier uit de registratie verwijderd c.q. vernietigd. Gegevens die niet vallend onder wetgeving worden niet langer bewaard dan nodig is.

**Beschermen van Persoonsgegevens**
We treffen beveiligingsmaatregelen om uw persoonlijke gegevens te beschermen tegen ongeautoriseerde toegang, wijziging of vernietiging.

Zo sluiten wij (verwerkers)een overeenkomst met eventuele derde partijen af, die namens ons gegevens verwerken. Daarbij adequate beveiligingsmaatregelen treffen om uw gegevens volgens de privacywetgeving te beschermen tegen verlies en onrechtmatige verwerking. Deze maatregelen zijn in overeenstemming met de voor de zorgsector geldende beveiligingsnormen, zoals vastgelegd in de NEN7510

De wet schrijft voor dat zorginstellingen moeten voldoen aan deze NEN7510 norm- Informatiebeveiliging in de zorg.

Met het **informatiebeveiligingsbeleid** wordt door de organisatie invulling gegeven aan de NEN-norm 7510 en de NIS2, cybersecurity.

**Datalekken**
De organisatie behandeld datalekken middels de procedure Melden Datalek
Indien er sprake is van ernstig nadelige gevolgen dan wel sprake is van ernstig nadelige gevolgen voor de bescherming van persoonsgegevens maakt de organisatie van het datalek een melding aan de AP.

**Klachten gerelateerd aan de verwerking van persoonsgegevens**
Klacht omtrent de verwerking van persoonsgegevens en de bescherming van de privacy van de cliënten worden behandeld via de Klachtenprocedure Privacy van de organisatie en kunnen per mail worden ingediend privacy@mij.nl

**Interne Informatiebeveiliging Privacy Adviseur (IPA)**
De organisatie heeft een Interne Privacy Adviseur(IPA) die de organisatie ondersteund bij de uitvoering van de Algemene Verordening Gegevensbescherming (AVG) en de NEN 7510. Beantwoord vragen van cliënten en medewerkers en biedt begeleiding bij Informatiebeveiliging en privacygerelateerde kwesties, zoals gegevensverzameling, gegevensopslag, gegevensuitwisseling en gegevensverwerking. Vragen met betrekking op Privacy en Informatiebeveiliging kunnen worden gesteld per mail privacy@mij.nl

**Functionaris gegevens bescherming (FG)**
De organisatie heeft een externe functionaris gegevensbescherming die erop toeziet dat de privacywetgeving binnen de organisatie wordt nageleefd. Heeft u vragen of opmerkingen over deze privacyverklaring of over de manier waarop wij uw gegevens verwerken, dan kunt u contact opnemen met de functionaris gegevensbescherming.

De contactgegevens vindt u op onze website

**Definities**

**AVG:** Algemene Verordening Gegevensbescherming
**Betrokkene:** Een geïdentificeerd of identificeerbaar natuurlijk persoon op wie een Persoonsgegeven betrekking heeft

**Bijzondere persoonsgegevens:** Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid, zoals bedoeld in artikel 9 AVG

**Datalek:** Een inbreuk op de beveiliging van Persoonsgegevens, die per ongeluk of opzettelijk leidt tot de vernietiging, het verlies, de wijziging of ongeoorloofde toegang tot die gegevens.

**Derde:** Een partij, niet zijnde de Betrokkene, noch de Verwerkingsverantwoordelijke, noch de Verwerker, noch enig persoon die onder rechtstreeks gezag valt van de Verwerkingsverantwoordelijke of de Verwerker, die gemachtigd is om Persoonsgegevens te verwerken

**Verwerking**: Elke handeling of geheel van handelingen met betrekking tot Persoonsgegevens, waaronder het verzamelen, vastleggen, ordenen, opslaan, raadplegen, bijwerken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, afschermen, wissen of vernietigen van gegevens.

**Verwerker**: Een partij die ten behoeve van en op instructie van de organisatie persoonsgegevens verwerkt

**Verwerking**: Elke handeling of geheel van handelingen met betrekking tot Persoonsgegevens, waaronder het verzamelen, vastleggen, ordenen, opslaan, raadplegen, bijwerken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, afschermen, wissen of vernietigen van gegevens.