Privacybeleid cliënten
Zorgvuldig en transparant omgaan met persoonsgegevens

Classificatie: Openbaar (extern beschikbaar)

1. Doel en uitgangspunten

MIJ verwerkt persoonsgegevens van cliënten om goede, veilige en verantwoorde zorg te kunnen bieden. Dit privacybeleid beschrijft welke uitgangspunten MIJ toepast, voor welke doelen persoonsgegevens worden verwerkt, hoe deze gegevens worden beschermd en welke rechten cliënten hebben.
Rechtmatigheid, behoorlijkheid en transparantie: persoonsgegevens worden alleen verwerkt als daarvoor een geldige grondslag bestaat en cliënten worden hierover begrijpelijk geïnformeerd.
Doelbinding: persoonsgegevens worden alleen gebruikt voor vooraf bepaalde en gerechtvaardigde doelen.
Dataminimalisatie: MIJ verwerkt niet meer persoonsgegevens dan noodzakelijk.
Juistheid: persoonsgegevens worden waar nodig geactualiseerd.
Bewaarbeperking: persoonsgegevens worden niet langer bewaard dan noodzakelijk of wettelijk verplicht.
Integriteit en vertrouwelijkheid: MIJ treft passende technische en organisatorische maatregelen.
Verantwoordingsplicht: MIJ kan aantonen dat de AVG-beginselen worden nageleefd.

2. Reikwijdte

Dit beleid is van toepassing op alle geheel of gedeeltelijk geautomatiseerde verwerkingen en op papieren of digitale bestanden met persoonsgegevens van cliënten die zorg van MIJ ontvangen, hebben ontvangen of willen ontvangen. Het geldt voor medewerkers, vrijwilligers, stagiairs, ingehuurde professionals en externe partijen die namens MIJ persoonsgegevens verwerken. Voor persoonsgegevens van medewerkers geldt het **Privacy HR-beleid.**

3. Wet- en regelgeving

MIJ verwerkt persoonsgegevens in overeenstemming met de toepasselijke wet- en regelgeving. De belangrijkste kaders zijn:

- Algemene verordening gegevensbescherming (AVG) en Uitvoeringswet AVG (UAVG)
- Wet op de geneeskundige behandelingsovereenkomst (WGBO)
- Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz)
- Wet elektronische gegevensuitwisseling in de zorg (Wegiz)
- Wet langdurige zorg (Wlz)
- Wet maatschappelijke ondersteuning (Wmo)
- Zorgverzekeringswet (Zvw)
- Wet kwaliteit, klachten en geschillen zorg (Wkkgz)
- Wet zorg en dwang (Wzd)
- Europese Network and Information Systems-richtlijn (NIS2
- NEN 7510 en aanverwante normen voor informatiebeveiliging in de zorg, voor zover van toepassing

Andere wet- en regelgeving wordt toegepast wanneer die voor een specifieke verwerking relevant is. Gedetailleerde wettelijke grondslagen, bewaartermijnen en verwerkingen worden vastgelegd in het verwerkingsregister en onderliggende procedures.

4. Verantwoordelijkheden

Raad van Bestuur: is eindverantwoordelijk voor de naleving van privacywetgeving en stelt dit beleid vast.
Leidinggevenden: zorgen voor toepassing van dit beleid binnen hun teams en nemen passende maatregelen bij afwijkingen.
Medewerkers en andere gebruikers: verwerken persoonsgegevens uitsluitend voor hun taak, volgen instructies, houden gegevens geheim en melden incidenten direct.
Interne Privacy Adviseur (IPA): adviseert en ondersteunt de organisatie bij privacy en informatiebeveiliging en coördineert privacyverzoeken en incidenten.
Functionaris voor gegevensbescherming (FG): houdt onafhankelijk toezicht op de naleving van de privacywetgeving en adviseert de organisatie.

5. Welke persoonsgegevens verwerkt MIJ?
Onder verwerking wordt verstaan elke handeling met betrekking tot persoonsgegevens.
De wet noemt als voorbeelden van verwerking:

- Het verzamelen, Opvragen, Raadplegen, Gebruiken, Vastleggen
- Bijwerken, Wijzigen, Ordenen, 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

Categorie	Voorbeelden	Mogelijke doelen
Identificatie en contactgegevens	Naam, adres, geboortedatum, contactgegevens, BSN voor zover wettelijk toegestaan, vertegenwoordiger en eerste contactpersoon	Identificatie, communicatie, administratie en uitvoering van zorg
Zorg en gezondheidsgegevens	Diagnoses, medicatie, allergieën, behandel en ondersteuningsgegevens, overdrachten, incidenten en relevante (wond) foto's.	Zorgverlening, dossiervoering, continuïteit, kwaliteit en veiligheid
Financiële en verzekeringsgegevens	Verzekering, polisnummer en rekeningnummer indien van toepassing	Declaratie, facturatie en wettelijke administratie
Beeld en toegangsgegevens	Camerabeelden en toegangsregistraties voor zover toegepast	Beveiliging van cliënten, medewerkers, bezoekers en eigendommen
Digitale gegevens	Technische gegevens en cookies voor zover via de website verwerkt	Werking, beveiliging en verbetering van digitale diensten

6. Doelen en grondslagen
MIJ verwerkt persoonsgegevens alleen voor concrete doelen en op basis van een geldige grondslag. Afhankelijk van de verwerking kan dit zijn: uitvoering van een overeenkomst, een wettelijke verplichting, bescherming van vitale belangen, een taak van algemeen belang, een gerechtvaardigd belang of toestemming. Voor gezondheidsgegevens is daarnaast een uitzondering op het verbod van artikel 9 AVG vereist, bijvoorbeeld omdat verwerking noodzakelijk is voor het verlenen of beheren van gezondheidszorg.
Belangrijke verwerkingsdoelen zijn onder meer:

- Het leveren, coördineren en evalueren van zorg en ondersteuning
- Het aanleggen en bijhouden van het cliëntdossier
- Communicatie met de cliënt, vertegenwoordiger en betrokken zorgverleners
- Administratie, declaratie en financiële afhandeling
- Kwaliteitsbewaking, incident- en calamiteitenonderzoek en cliënttevredenheidsonderzoek
- Beveiliging van personen, gebouwen, systemen en eigendommen
- Het voldoen aan wettelijke verplichtingen

7. Herkomst, toegang en verstrekking

7.1 Herkomst

Persoonsgegevens worden verkregen van de cliënt, diens wettelijk vertegenwoordiger of contactpersoon, en van bevoegde zorgverleners of instanties wanneer daarvoor een geldige grondslag bestaat. MIJ gaat niet automatisch uit van toestemming. Per gegevensuitwisseling wordt beoordeeld welke grondslag en eventuele wettelijke geheimhoudingsregels gelden.

7.2 Toegang

Toegang tot gegevens, wordt verstrekt op basis van rol, functie en noodzaak voor de taakuitoefening. Autorisaties worden periodiek gecontroleerd. Gebruikers zijn gebonden aan geheimhouding. Externe toegang is alleen toegestaan wanneer die noodzakelijk, beveiligd en contractueel vastgelegd is.

7.3 Verstrekking aan derden

MIJ verstrekt persoonsgegevens uitsluitend wanneer dit noodzakelijk is voor de zorgverlening, een wettelijke verplichting, een andere geldige grondslag of wanneer de cliënt rechtsgeldig toestemming heeft gegeven. Ontvangers kunnen onder meer zorgkantoren, gemeenten, het CAK, het CIZ, toezichthouders, behandelaren, leveranciers en een meetbureau zijn. De concrete ontvangers en grondslagen worden opgenomen in het verwerkingsregister en de privacyverklaring. MIJ verkoopt persoonsgegevens niet en verstrekt deze niet voor commerciële marketingdoeleinden.
Met partijen die namens MIJ persoonsgegevens verwerken worden passende verwerkersafspraken gemaakt. Gegevensuitwisseling vindt plaats via goedgekeurde en beveiligde kanalen.

8. Gebruik van kunstmatige intelligentie (AI)

MIJ kan goedgekeurde AI-toepassingen gebruiken ter ondersteuning van werkzaamheden, bijvoorbeeld bij het structureren, samenvatten of opstellen van teksten. Wanneer daarbij persoonsgegevens worden verwerkt, gelden onverkort de AVG, dit privacybeleid, het AI-beleid en de interne beveiligings- en autorisatieregels.

- AI ondersteunt medewerkers maar neemt niet zelfstandig besluiten die rechtsgevolgen hebben of cliënten anderszins in aanmerkelijke mate treffen, tenzij dit wettelijk is toegestaan en passende waarborgen zijn getroffen.
- AI-uitkomsten worden altijd door een bevoegde medewerker gecontroleerd op juistheid, volledigheid, passendheid en mogelijke vooringenomenheid.
- Vooraf wordt beoordeeld of opname in het verwerkingsregister, een DPIA en/of een beoordeling onder de AI-verordening nodig is.
- Cliënten worden begrijpelijk geïnformeerd wanneer AI een relevante rol speelt bij de verwerking van hun persoonsgegevens of bij besluitvorming die hen raakt.
- Invoer en uitvoer worden niet langer bewaard dan noodzakelijk en worden beschermd volgens de geldende classificatie en beveiligingsregels.
- Cliënten kunnen informatie vragen over de inzet van AI bij de verwerking van hun persoonsgegevens

MIJ maakt gebruik van goedgekeurde digitale hulpmiddelen, waaronder AI-toepassingen. Hierbij worden persoonsgegevens uitsluitend verwerkt indien hiervoor een geldige grondslag bestaat en passende technische en organisatorische maatregelen zijn getroffen. AI neemt geen zelfstandige besluiten over cliënten, indicaties, zorgverlening of andere zaken die rechtsgevolgen hebben of cliënten anderszins in aanmerkelijke mate treffen. Besluiten worden altijd genomen door een bevoegde medewerker.

9. Rechten van cliënten
Cliënten kunnen, voor zover de AVG dit recht geeft, gebruikmaken van:

- Recht op informatie
- Recht op inzage
- Recht op rectificatie
- Recht op gegevenswissing
- Recht op beperking van de verwerking
- Recht op overdraagbaarheid van gegevens
- Recht van bezwaar
- Recht om toestemming in te trekken, zonder dat dit de rechtmatigheid van eerdere verwerking aantast
- Recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens

Een verzoek kan worden ingediend via privacy@mij.nl MIJ kan om aanvullende informatie vragen om de identiteit van de verzoeker proportioneel vast te stellen. Verzoeken worden behandeld binnen de wettelijke termijnen. Wanneer een verzoek geheel of gedeeltelijk wordt afgewezen, motiveert MIJ dit.

10. Bewaren en vernietigen
MIJ bewaart persoonsgegevens niet langer dan wettelijk verplicht of noodzakelijk voor het doel waarvoor zij zijn verzameld. De bewaartermijnen zijn vastgelegd in het bewaarbeleid en/of verwerkingsregister. Voor zorgdossiers geldt in beginsel de wettelijke bewaartermijn van de WGBO, gerekend vanaf de laatste wijziging in het dossier, of langer wanneer dit redelijkerwijs uit de zorg van een goed hulpverlener voortvloeit. Na afloop van de bewaartermijn worden gegevens veilig vernietigd of geanonimiseerd, tenzij langer bewaren wettelijk verplicht of aantoonbaar noodzakelijk is.

11. Beveiliging en privacy by design
MIJ treft passende technische en organisatorische maatregelen, afgestemd op de aard van de gegevens en de risico's. Hieronder vallen onder meer autorisatie op basis van rol en functie, logging, sterke authenticatie, beveiligde gegevensuitwisseling, leveranciersafspraken, back-ups, bewustwording en periodieke controle. Bij nieuwe of gewijzigde processen en systemen worden privacy by design en privacy by default toegepast. Waar een verwerking waarschijnlijk een hoog privacyrisico oplevert, wordt vooraf een DPIA uitgevoerd.

12. Datalekken en incidenten
Een vermoeden van verlies, onjuiste verstrekking, ongeoorloofde toegang of een andere inbreuk op persoonsgegevens wordt direct intern gemeld volgens de procedure Melden van een Informatieveiligheids Incident of datalek. MIJ onderzoekt het incident, beperkt de gevolgen, legt de beoordeling vast en meldt het datalek waar nodig binnen de wettelijke termijn aan de Autoriteit Persoonsgegevens en/of aan betrokkenen.

13. Vragen en klachten
Vragen, verzoeken en privacyklachten kunnen worden gestuurd naar privacy@mij.nl Privacyklachten worden behandeld door Interne IB en Privacy Adviseur volgens de klachtenprocedure. De contactgegevens van de externe Functionaris Gegevensbescherming staan op de website van MIJ. Een cliënt behoudt het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens.

14. Beheer en evaluatie
Dit beleid wordt minimaal jaarlijks en daarnaast bij relevante wijzigingen in wetgeving, organisatie, systemen, gegevensverwerkingen of risico's geëvalueerd. Wijzigingen worden vastgesteld volgens het documentbeheerproces en gecommuniceerd aan betrokken medewerkers.

Kernbegrippen

Begrip	**Betekenis**
Betrokkene	De persoon op wie persoonsgegevens betrekking hebben.
Persoonsgegeven	Informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.
Bijzonder persoonsgegeven	Een extra beschermde categorie, waaronder gegevens over gezondheid, religie, afkomst en biometrische gegevens voor unieke identificatie.
Verwerking	Elke handeling met persoonsgegevens, zoals verzamelen, raadplegen, wijzigen, delen, bewaren, afschermen of verwijderen.
Verwerkingsverantwoordelijke	De organisatie die het doel en de middelen van de verwerking bepaalt.
Verwerker	Een partij die ten behoeve van en volgens instructies van MIJ persoonsgegevens verwerkt.
Datalek	Een beveiligingsinbreuk die leidt tot vernietiging, verlies, wijziging, ongeoorloofde verstrekking of ongeoorloofde toegang tot persoonsgegevens.
AI-systeem	Een systeem dat op basis van ingevoerde gegevens output genereert, zoals voorspellingen, aanbevelingen, inhoud of beslissingen.