Psychologenpraktijk Marion Roosen
psychologische en pedagogische hulpverlening

postadres
Postbus 121
5060 AC Oisterwijk

praktijkadres
Enschotsestraat 126
5014 DJ Tilburg
06 - 16 97 11 13

e-mail
info@ppmr.nl
website
www.ppmr.nl

kamer van koophandel
17273058
bankrekeningnummer
NL29 INGB 0750 6838 56

AGB-code praktijk
94 - 05 76 47
AGB-code zorgverlener
94 - 00 90 80

INTERN PRIVACYBELEID MHF Roosen (PPMR)

1. Inleiding

Dit is het privacybeleid van MHF Roosen (Psychologen Praktijk M. Roosen/PPMR). Dit privacybeleid heeft betrekking op het verwerken van (bijzondere) persoonsgegevens in het kader van zowel de zorgverlening als de (interne) bedrijfsvoering van PPMR.

MHF Roosen is als zorgaanbieder verwerkingsverantwoordelijke. MHF Roosen hierna genoemd als PPMR.
PPMR bepaalt het doel en de middelen voor de verwerking van (bijzondere) persoonsgegevens. Dit document beschrijft de wijze waarop MHF Roosen/PPMR als verwerkingsverantwoordelijke met (bijzondere) persoonsgegevens omgaat, zodat aan de vereisten van de Algemene verordening gegevensbescherming ('AVG') wordt voldaan.

Aan bod komen de volgende onderwerpen:

2. Actualisatie en controle naleving privacybeleid;
3. Categorieën persoonsgegevens en doelen;
4. Organisatorische en technische maatregelen / beveiliging;
5. Informatieplicht;
6. Verwerkingsregister;
7. Verwerkers en ontvangers;
8. Bewaartermijnen;
9. Vooralsnog geen gegevensbeschermingseffectbeoordeling (DPIA);
10. Doorgifte buiten de EU;
11. Geen functionaris voor de gegevensbescherming;
12. Beveiligingsincidenten;
13. Rechten van betrokkenen.

2. Actualisatie en controle naleving privacybeleid

De verwerking van persoonsgegevens binnen PPMR dient in overeenstemming te blijven met de AVG en met elke verordening en wet- en regelgeving die de AVG aanvult, wijzigt of vervangt. Om die reden zal het privacybeleid periodiek worden geëvalueerd en zo nodig worden aangepast. Eveneens zal periodiek worden gecontroleerd of het privacybeleid door medewerkers en verwerkers van PPMR daadwerkelijk wordt nageleefd.

3. Categorieën persoonsgegevens en verwerkingsdoelen

PPMR verwerkt persoonsgegevens van de volgende categorieën personen:
a. (potentiële) patiënten;
b. bezoekers aan het praktijkpand van PPMR;
c. bezoekers van ppmr.nl (website);
d. zpp'ers;
e. sollicitanten;
f. alle overige personen die met PPMR contact opnemen of van wie PPMR persoonsgegevens verwerkt.

a. <u>(potentiële) patiënten</u>

PPMR verwerkt persoonsgegevens van (potentiële) patiënten, ten behoeve van identificatie van de patiënt en de uitvoering van de behandelovereenkomst. Voor identificatie gaat het om naam, contact- en adresgegevens, geboortedatum en kenmerk van het identiteitsbewijs en BSN van de patiënt. Voor de uitvoering van de behandelovereenkomst gaat het ook om andere (bijzondere) persoonsgegevens, zoals medische gegevens.

De opgenomen gegevens van een patiënt worden in het ICT-systeem van PPMR opgeslagen.

b. bezoekers aan de praktijk van PPMR
Er worden bij bezoekers aan de praktijk geen registraties of camerabeelden gemaakt.

c. bezoekers van ppmr.nl (website)
Er worden geen cookies via de website verzameld.

Verder worden persoonsgegevens gegenereerd als een bezoeker een contact- of ander webformulier op de website invult. Dit formulier is beveiligd. Die gegevens worden gebruikt voor het doel waarvoor het contact- of webformulier dient.

d. zzp'ers
PPMR verwerkt de persoonsgegevens van door haar ingeschakelde zzp'ers. PPMR vraagt zzp'ers niet om een kopie of scan van hun identiteitsbewijs te verstrekken. Wel zal in het kader van de vergewisplicht (Wkkgz) een onderzoek worden gedaan naar de geschiktheid van de zzp'er.

e. sollicitanten
Van personen die bij PPMR hebben gesolliciteerd, worden persoonsgegevens verwerkt, zoals contactgegevens en gegevens die zijn vermeld in de sollicitatiebrief en het cv. Deze gegevens worden verwerkt ter beoordeling van de geschiktheid van de kandidaat en om met een kandidaat contact te leggen. De gegevens worden bewaard tot maximaal 6 maanden na de sollicitatieprocedure.

f. overige personen
In het kader van de behandeling, kan PPMR ook gebruikmaken van gegevens afkomstig van andere hulpverleners mits schriftelijke toestemming van betreffende cliënt enkel en alleen als gaat om inwinnen van informatie van vorige behandeling.

4. Organisatorische en technische maatregelen / beveiliging

Uitgangspunt voor PPMR is dat niet meer persoonsgegevens worden verwerkt dan noodzakelijk is om het doel te bereiken waarvoor ze zijn verzameld, zowel intern als bij inschakeling van derde partijen. Voor beide gevallen heeft PPMR passende technische en organisatorische maatregelen getroffen om persoonsgegevens te beschermen tegen verlies of onrechtmatige verwerking.

Interne maatregelen
PPMR heeft de volgende interne technische en organisatorische maatregelen getroffen:

a. het uitwisselen van vertrouwelijke informatie met andere zorgverleners dient (conform NEN 7510, NEN 7512 en NEN 7513) uitsluitend via een beveiligde verbinding (versleuteld mailverkeer, portaal via EPD, Praktijkdata) plaats te vinden. E-mailen met andere hulpverleners is alleen toegestaan voor algemene communicatie. Uitwisseling van vertrouwelijke informatie via (zakelijke of privé) e-mailaccounts van medewerkers of via applicaties als WhatsApp, Dropbox of WeTransfer is niet toegestaan;

b. vertrouwelijke informatie dient uitsluitend te worden opgeslagen in het ICT-systeem van de praktijk dat voldoet aan NEN 7510, NEN 7512 en NEN 7513 en niet daarbuiten. Het is ook niet toegestaan vertrouwelijke informatie naar externe gegevensdragers te kopiëren, tenzij dit noodzakelijk is en deze gegevens zijn versleuteld;

c. iedere medewerker draagt ervoor zorg dat zijn/haar wachtwoord voor het ICT-systeem van de praktijk voldoende sterk is en periodiek wordt gewijzigd;

d. het is niet toegestaan apparatuur als laptops, tablets en mobiele telefoons onbeheerd buiten de praktijk achter te laten. Toegang tot dergelijke apparatuur dient te zijn afgeschermd met een wachtwoord;

e. inloggegevens dienen vertrouwelijk te worden behandeld en dienen niet met derden te worden gedeeld. Uitsluitend in voorkomende gevallen mogen inloggegevens vertrouwelijk met een collega worden gedeeld, zoals in geval van waarneming tijdens verlof of langdurige ziekte;

f. bij (dagelijks) vertrek van de praktijk dient iedere medewerker zijn/haar desktop computer volledig uit te loggen, af te sluiten en eventuele papieren dossiers volledig en veilig op te bergen;

g. het is niet toegestaan, zonder toestemming van PPMR, software te downloaden en/of om firewalls of virusscanners aan te passen of te verwijderen;

h. een thuiscomputer van de zorgaanbieder zelf of van een medewerker waarmee verbinding wordt gemaakt met het netwerk van de praktijk (VPN-verbinding) dient te zijn voorzien van actieve wachtwoordbeveiliging, firewall en virusscanner. Veiligheidsupdates dienen tijdig te worden uitgevoerd. Er mag geen verbinding worden gelegd via openbare wifi-netwerken. Het is niet toegestaan vertrouwelijke informatie op de thuiscomputer op te slaan of om papieren dossiers of externe gegevensdragers (zoals een laptop, tablet of externe harde schijn) met vertrouwelijke informatie onbeheerd in een auto of elders buiten de praktijk achter te laten;

i. bij vertrek van de praktijk dient iedere medewerker te controleren of er nog andere medewerkers in het pand aanwezig zijn. De laatst aanwezige medewerker zorgt ervoor dat alle ramen en deuren zijn gesloten;

j. toegang tot het pand is alleen mogelijk met aan medewerkers verstrekte sleutels. Sleutels mogen niet aan derden worden afgegeven;

k. personeel/ZZP'ers is contractueel verplicht tot geheimhouding.

PPMR ziet op naleving van de hiervoor genoemde maatregelen. Steekproefsgewijs kunnen (proportionele) controles worden uitgevoerd. Als wordt vermoed dat maatregelen door een bepaalde medewerker niet in acht worden genomen, kan worden overgegaan tot gerichte controles tegen de medewerker in kwestie. Na deze controle kan PPMR op basis van haar bevindingen besluiten tot het treffen van arbeidsrechtelijke maatregelen.

Verwerkers
Met verwerkers heeft PPMR afspraken gemaakt over de te nemen technische en organisatorische maatregelen. Op grond van de vastgestelde risico's die de persoonsgegevens en de aard van de verwerking met zich meebrengen, is het gewenste beveiligingsniveau bepaald.

Door PPMR ingeschakelde verwerkers zijn verplicht PPMR alle informatie te verstrekken die nodig is om de nakoming van de verplichtingen als verwerker aan te tonen en audits, waaronder inspecties, door PPMR of een door PPMR gemachtigde controleur mogelijk te maken en er aan bij te dragen.

5. Informatieplicht

PPMR informeert betrokkenen over hoe met persoonsgegevens wordt omgegaan. Voor personen die niet aan PPMR zijn verbonden, is om die reden een extern privacystatement opgesteld. Dit privacystatement is op de website van PPMR gepubliceerd.

Bij indiensttreding (ZZP) worden nieuwe medewerkers geïnformeerd over de verwerking van hun persoonsgegevens binnen PPMR. Voor medewerkers geldt een intern privacyprotocol. Dit interne protocol van PPMR is opgenomen in het ICT-systeem van de praktijk.

6. Verwerkingsregister

PPMR houdt een verwerkingsregister bij. Dit register bevat een beschrijving van onder meer de verwerkingsdoeleinden, categorieën betrokkenen en ontvangers, bewaartermijnen en beveiligingsmaatregelen. In het verwerkingsregister worden verwerkingsactiviteiten per categorie betrokkene en per categorie persoonsgegeven bijgehouden.

Het verwerkingsregister (Excel-bestand) is opgenomen in het ICT-systeem van de praktijk.

7. Verwerkers en ontvangers

Verwerkers
PPMR kan bij het verwerken van persoonsgegevens gebruikmaken van externe dienstverleners. Deze dienstverleners verwerken uitsluitend persoonsgegevens op instructie van PPMR. Met deze partijen heeft PPMR verwerkersovereenkomsten gesloten. In deze overeenkomsten zijn afspraken vastgelegd over onder meer de aard en doeleinden van de verwerking, het soort persoonsgegevens dat wordt verwerkt, geheimhoudingsplicht, instructies over de verwerking, beveiligingsmaatregelen, het al dan niet inschakelen van subverwerkers, privacyrechten van betrokkenen, audits en controle alsook het retourneren en/of verwijderen van persoonsgegevens door de verwerker.

PPMR maakt gebruik van de volgende verwerkers:

- Boekhouding: Accountantskantoor Kwadrant te Oisterwijk in de persoon van dhr. P. Hamers
- EPD: Praktijkdata/Telasoft in de persoon van dhr. M. de Ruiter

Ontvangers
PPMR verstrekt persoonsgegevens van betrokkenen aan derden wanneer dat noodzakelijk is in het kader van de uitvoering van de behandelovereenkomst, de uitvoering van een (arbeids)overeenkomst of in geval van een wettelijke verplichting. Daarbuiten worden geen persoonsgegevens aan derden verstrekt zonder voorafgaande uitdrukkelijke toestemming van de betrokkene.

8. Bewaartermijnen
PPMR vernietigt persoonsgegevens die niet langer noodzakelijk zijn voor het doel waarvoor ze zijn verzameld en tevens niet op grond van andere wetgeving bewaard moeten worden. De persoonsgegevens worden in dat geval verwijderd.

PPMR hanteert in beginsel de volgende bewaartermijnen:

a. medische gegevens: ten minste 15 jaar na het einde van de behandelovereenkomst;
b. (financieel-)administratieve gegevens: 7 jaar na vastlegging van de gegevens;
c. gegevens van medewerkers en zzp'ers, anders dan (financieel-)administratieve gegevens: 5 jaar na uitdiensttreding respectievelijk na het einde van de overeenkomst van opdracht;
d. gegevens van sollicitanten: 6 maanden na afronding van de sollicitatieprocedure;
e. bezoekers van de website en ontvangers van nieuwsbrieven: 5 jaar na het laatste bezoek aan de website respectievelijk na uitschrijving voor de nieuwsbrief, tenzij eerder bezwaar wordt gemaakt in welk geval tot vernietiging zal worden overgegaan.

9. Vooralsnog geen gegevensbeschermingseffectbeoordeling (DPIA)
In uitzonderingsgevallen zou sprake kunnen zijn van het uitvoeren van een DPIA. In dat geval voert PPMR voor elke nieuwe verwerking van persoonsgegevens een DPIA uit, indien deze een hoog risico voor de rechten en vrijheden van natuurlijke personen inhoudt, gelet op de aard, de omvang, de context en de doeleinden daarvan.

10. Doorgifte buiten EER
PPMR geeft in beginsel geen persoonsgegevens door aan landen buiten de Europese Economische Ruimte (EER). Indien dit toch noodzakelijk mocht zijn, draagt PPMR ervoor zorg dat de doorgifte

alleen plaatsvindt als de Europese Commissie heeft aangegeven dat het betreffende land een passend beschermingsniveau biedt of als sprake is van passende waarborgen in de zin van de AVG.

11. Geen functionaris voor de gegevensbescherming

Een verwerkingsverantwoordelijke dient een functionaris voor de gegevensbescherming (FG) aan te wijzen, onder meer in geval deze hoofdzakelijk is belast met grootschalige verwerking van bijzondere persoonsgegevens (zoals medische gegevens). 'Hoofdzakelijk belast' heeft betrekking op de kernactiviteiten van de verwerkingsverantwoordelijke. De Artikel 29-werkgroep definieert kernactiviteiten als processen die essentieel zijn om de doelen van de organisatie te bereiken, of die tot de hoofdtaken van de organisatie horen.

PPMR heeft geen FG aangesteld aangezien **geen** sprake is van een grootschalige verwerking van bijzondere persoonsgegevens (zie handleiding).

12. Beveiligingsincidenten

PPMR heeft passende technische en organisatorische maatregelen genomen die tot doel hebben de kans op verlies of onrechtmatige verwerking van persoonsgegevens zo veel mogelijk te beperken. Ondanks deze maatregelen bestaat de kans dat zich toch een incident met betrekking tot persoonsgegevens voordoet. Om ervoor te zorgen dat er zo snel mogelijk opgetreden kan worden om het incident te beëindigen en de schade zo veel mogelijk te beperken, dient als volgt te worden gehandeld.

Bij elk incident met betrekking tot persoonsgegevens zal PPMR beoordelen:

- of sprake is van een incident dat betrekking heeft op (bijzondere) persoonsgegevens;
- welke maatregelen genomen moeten worden om het incident te beëindigen en de gevolgen te beperken;
- of inschakeling van een externe partij is benodigd om bij de oplossing van het incident te assisteren;
- of het incident aan de AP dient te worden gemeld;
- of degenen op wie de persoonsgegevens betrekking hebben, over het incident dienen te worden ingelicht;
- welke maatregelen er genomen moeten worden om herhaling van het incident te voorkomen.

PPMR documenteert alle inbreuken in verband met persoonsgegevens in het datalekkenregister.

Voor het geval dat een (potentieel) incident waarvan een door PPMR ingeschakelde verwerker eerder op de hoogte is geraakt, is in de verwerkersovereenkomst bepaald dat de verwerker PPMR zo snel mogelijk bericht. Ook zijn er afspraken gemaakt over het oplossen van het incident en het verstrekken van nadere gegevens.

13. Rechten van betrokkenen

Rechten die een betrokkene volgens de AVG in zijn algemeenheid heeft, zijn het recht van inzage, het recht op rectificatie, het recht op gegevenswissing, het recht op beperking van de verwerking, het recht op overdraagbaarheid, het recht van bezwaar en het recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming. PPMR heeft zodanige technische maatregelen genomen dat aan een gerechtvaardigde uitoefening van deze rechten gevolg kan worden gegeven.

Verzoeken van betrokkenen met betrekking tot persoonsgegevens worden door mw. M. Roosen, GZ-psycholoog afgewikkeld.

Verzoeken en de afhandeling daarvan worden opgeslagen in een afzonderlijke map in het ICT-systeem.

Na ontvangst van een verzoek zal PPMR eerst de identiteit van de verzoeker vaststellen, aan de hand van naam, contact- en adresgegevens, identiteitsbewijs en geboortedatum.

Nadat de identiteit van de verzoeker is vastgesteld, zal PPMR aan de verzoeker bevestigen dat er binnen één maand op het verzoek zal worden gereageerd. Als blijkt dat het verzoek complex is,

kan deze termijn met maximaal twee maanden worden verlengd. Over verlenging van de termijn informeert PPMR de verzoeker binnen de eerste maand.

PPMR stelt vast welk recht de verzoeker inroept en verzamelt in dat kader de benodigde gegevens. PPMR beoordeelt of aan het verzoek van de verzoeker kan worden voldaan, mede gelet op het beroepsgeheim en de wettelijke bewaarplicht. De behandelaar legt zijn bevindingen in een verslag vast. Het verslag wordt opgeslagen in een map van het ICT-systeem van de praktijk, dat speciaal voor het verzoek is aangelegd.

In beginsel worden aan de verzoeker voor de behandeling van het verzoek **geen** kosten in rekening gebracht. Niettemin kan de verzoeker een redelijke vergoeding op basis van de administratieve kosten in rekening worden gebracht, bijvoorbeeld in geval van herhaalde (ongegronde) verzoeken of als meer dan één kopie van een dossier wordt verlangd.

Als het verzoek wordt gehonoreerd en het verzoek heeft betrekking op rectificatie, wissing of beperking van de verwerking, dienen ook de externe partijen die de persoonsgegevens hebben ontvangen van het verzoek in kennis te worden gesteld. PPMR stelt vast of daarvan sprake is en noteert de derde partijen in zijn verslag. Dergelijke kennisgevingen aan externe partijen laat PPMR achterwege als dit onmogelijk blijkt of onevenredig veel inspanning vergt.