

Intern privacy beleid MeJa

1. Inleiding

Dit is het privacy beleid van MeJa. Dit privacy beleid heeft betrekking op het verwerken van (bijzondere) persoonsgegevens in het kader van zowel de zorgverlening als de (interne) bedrijfsvoering van MeJa.

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

Aan bod komen de volgende onderwerpen:

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

2. Actualisatie en controle naleving privacy beleid

De verwerking van persoonsgegevens binnen MeJa 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 privacy beleid periodiek worden geëvalueerd en zo nodig worden aangepast. Eveneens

zal periodiek worden gecontroleerd of het privacy beleid door medewerkers en verwerkers van MeJa daadwerkelijk wordt nageleefd.

3. Categorieën persoonsgegevens en verwerkingsdoelen

MeJa verwerkt persoonsgegevens van de volgende categorieën personen:

- a. Bezoekers aan het praktijkpand van MeJa;
 - b. Bezoekers van www.meja-psychologie.nl;
 - c. Deelnemers aan bijeenkomsten van MeJa;
 - d. Sollicitanten;
 - e. (Potentiële) cliënten
 - f. Alle overige personen die met MeJa contact opnemen of van wie MeJa persoonsgegevens verwerkt.
- a. (Potentiële) cliënten

MeJa 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 cliënt worden in het ICT-systeem van opgeslagen.

- b. bezoekers van www.meja-psychologie.nl

Wanneer u onze website bezoekt, kunnen wij een aantal gegevens verwerken via cookies. Een cookie is een eenvoudig klein bestandje dat met pagina's van deze website [en/of Flash- applicaties] wordt meegestuurd en door uw browser op uw harde schrijf van uw computer wordt opgeslagen. De daarin opgeslagen informatie kan bij een volgend bezoek weer naar onze servers teruggestuurd worden. U kunt het gebruik van deze cookies weigeren, maar omdat dit de functionaliteit en de gebruikerservaring ernstig belemmert, en wij daarom niet de kwaliteit kunnen bieden die u van ons mag verwachten, hebben wij ervoor gekozen om u de website dan niet aan te bieden. Naast functionele cookies die bedoeld zijn om onze website goed te laten werken, kan ook sprake zijn van overige of onvoorziene cookies. Door de manier waarop internet en websites werken, kan het zijn dat wij niet altijd inzicht hebben in de cookies die via onze website door derde partijen worden geplaatst. Dit is met name het geval als onze webpagina's zogenaamde embedded elementen bevatten; dit zijn teksten, documenten, plaatjes of filmpjes die bij een andere partij opgeslagen zijn, maar die op, in of via onze website getoond worden.

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.

e. Sollicitanten

Van personen die bij MeJa 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 MeJa ook gebruikmaken van gegevens afkomstig van andere hulpverleners.

4. Organisatorische en technische maatregelen/ beveiliging

Uitgangspunt voor MeJa 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 MeJa passende technische en organisatorische maatregelen getroffen om persoonsgegevens te beschermen tegen verlies of onrechtmatige verwerking.

Interne maatregelen

MeJa heeft de volgende interne technische en organisatorische maatregelen getroffen:

- Het uitwisselen van vertrouwelijke informatie met andere zorgverleners wordt (conform NEN 7510, NEN 7512 en NEN 7513) uitsluitend via een beveiligde verbinding (versleuteld mailverkeer, zoals zorgmail of ZIVVER) uitgewisseld. 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;
- Vertrouwelijke informatie wordt uitsluitend opgeslagen in het ICT-systeem van de praktijk dat voldoet aan NEN 7510, NEN 7512 en NEN 7513 en niet daarbuiten. Vertrouwelijke informatie naar externe gegevensdragers gebeurt alleen als de gegevens zijn versleuteld en als dit noodzakelijk is.
- Het wachtwoord voor het ICT-systeem van de praktijk is voldoende sterk is en wordt periodiek gewijzigd;
- Apparatuur als laptops, tablets en mobiele telefoons worden niet onbeheerd buiten de praktijk achtergelaten. Toegang tot dergelijke apparatuur is afgeschermd met een wachtwoord;
- Inloggegevens worden vertrouwelijk behandeld en worden niet met derden gedeeld. Uitsluitend in voorkomende gevallen worden inloggegevens vertrouwelijk met een collega gedeeld, zoals in geval van waarneming tijdens verlof;
- Bij (dagelijks) vertrek van de praktijk wordt de computer volledig uitgelogd, afgesloten en eventuele papieren dossiers worden volledig en veilig opgeborgen;

- Het is niet toegestaan, zonder toestemming van MeJa, software te downloaden en/of om firewalls of virusscanners aan te passen of te verwijderen;
- Het netwerk van de praktijk (VPN-verbinding) is voorzien van actieve wachtwoordbeveiliging, firewall en virusscanner. Veiligheidsupdates worden tijdig uitgevoerd. Er wordt geen verbinding gelegd via openbare wifi-netwerken.
- 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 en dat het alarm wordt geactiveerd;
- Toegang tot het pand is alleen mogelijk met aan medewerkers verstrekte sleutels. Sleutels worden niet aan derden afgegeven;
- Personeel is contractueel verplicht tot geheimhouding.

MeJa 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 MeJa op basis van haar bevindingen besluiten tot het treffen van arbeidsrechtelijke maatregelen.

Verwerkers

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

5. Informatieplicht

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

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

6. Verwerkingsregister

MeJa 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 persoonsgegevens bijgehouden.

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

7. Verwerkers en ontvangers

Verwerkers

MeJa kan bij het verwerken van persoonsgegevens gebruikmaken van externe dienstverleners. Deze dienstverleners verwerken uitsluitend persoonsgegevens op instructie van MeJa. Met deze partijen heeft MeJa 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.

MeJa maakt gebruik van de volgende verwerkers: - Epos Zilos

Ontvangers

MeJa 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

MeJA 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.

MeJA hanteert in beginsel de volgende bewaartermijnen:

- Medische gegevens: ten minste 15 jaar na het einde van de behandelovereenkomst;
- (Financieel-)administratieve gegevens: 7 jaar na vastlegging van de gegevens;
- Gegevens van medewerkers en zzp'ers, anders dan (financieel-)administratieve gegevens: 5 jaar na uitdiensttreding respectievelijk na het einde van de overeenkomst van opdracht;
- Gegevens van sollicitanten: 6 maanden na afronding van de sollicitatieprocedure;
- 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 MeJa 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

MeJa geeft in beginsel geen persoonsgegevens door aan landen buiten de Europese Economische Ruimte (EER). Indien dit toch noodzakelijk mocht zijn, draagt MeJa 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.

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

12. Beveiligingsincidenten

MeJa 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 MeJa 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.

MeJa documenteert alle inbreuken in verband met persoonsgegevens in het datalekkenregister. Voor het geval dat een (potentieel) incident waarvan een door MeJa ingeschakelde verwerker eerder op de hoogte is geraakt, is in de verwerkersovereenkomst bepaald dat de verwerker MeJa 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. MeJa 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 M. Meek-Heekelaar, klinisch psycholoog of door K.E.Jager, klinisch psycholoog afgewikkeld. Verzoeken en de afhandeling daarvan worden opgeslagen in een afzonderlijke map in het ICT-systeem. Na ontvangst van een verzoek zal MeJa 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 MeJa 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 MeJa de verzoeker binnen de eerste maand.

MeJa stelt vast welk recht de verzoeker inroept en verzamelt in dat kader de benodigde gegevens. MeJa 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 (ongegrunde) 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. MeJa stelt vast of daarvan sprake is en noteert de derde partijen in zijn verslag. Dergelijke kennisgevingen aan externe partijen laat MeJa achterwege als dit onmogelijk blijkt of onevenredig veel inspanning vergt.