

INTERN PRIVACYBELEID Praktijk Psychologie Daphne Meijer

1. Inleiding

Dit is het privacybeleid van Daphne Meijer. Dit privacybeleid heeft betrekking op het verwerken van (bijzondere) persoonsgegevens in het kader van zowel de zorgverlening als de (interne) bedrijfsvoering van Daphne Meijer.

Daphne Meijer is als zorgaanbieder verwerkingsverantwoordelijke. Daphne Meijer bepaalt het doel en de middelen voor de verwerking van (bijzondere) persoonsgegevens. Dit document beschrijft de wijze waarop Daphne Meijer 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 Praktijk Psychologie van Daphne Meijer 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 verwerkers van Daphne Meijer daadwerkelijk wordt nageleefd.

3. Categorieën persoonsgegevens en verwerkingsdoelen

Daphne Meijer verwerkt persoonsgegevens van de volgende categorieën personen:

- a. (potentiële) patiënten;
- b. zzp'ers;
- c. alle overige personen die met Daphne Meijer contact opnemen of van wie Daphne Meijer persoonsgegevens verwerkt.

a. (potentiële) patiënten

Daphne Meijer 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 Daphne Meijer opgeslagen.

b. zzp'ers

Daphne Meijer verwerkt de persoonsgegevens van voor haar ingeschakelde zzp'ers. Daphne Meijer 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.

c. overige personen

In het kader van de behandeling, kan Daphne Meijer ook gebruikmaken van gegevens afkomstig van andere hulpverleners.

4. Organisatorische en technische maatregelen / beveiliging

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

Interne maatregelen

Daphne Meijer heeft de volgende interne technische en organisatorische maatregelen getroffen:

- a: Het uitwisselen van vertrouwelijke informatie wordt uitsluitend opgeslagen in het ICTsysteem van de praktijk dat voldoet aan NEN 7510, NEN 7512 en NEN 7513 en niet daarbuiten. Vertrouwelijke informatie wordt niet naar externe gegevensdragers gekopieerd, tenzij dit noodzakelijk is en deze gegevens zijn versleuteld;
- b: Daphne Meijer heeft een voldoende sterk wachtwoord voor het ICT-systeem van de praktijk welke periodiek wordt gewijzigd. Daarnaast is een 2e beveiliging ingesteld middels de mobiele telefoon van Daphne Meijer (tweefactor authenticatie);
- c: Apparatuur als laptops, tablets en mobiele telefoons worden niet onbeheerd buiten de praktijk achter gelaten. Toegang tot dergelijke apparatuur is afgeschermd met een wachtwoord;
- d: 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;
- e: bij (dagelijks) vertrek van de praktijk wordt de laptop volledig uitgelogd, afgesloten en eventuele papieren dossiers volledig en veilig opgeborgen;
- f: Veiligheidsupdates worden tijdig uitgevoerd. Er wordt geen verbinding gelegd via openbare wifi-netwerken. Er worden geen papieren dossiers of externe gegevensdragers (zoals een laptop, tablet of externe harde schijf) met vertrouwelijke informatie onbeheerd in een auto of elders buiten de praktijk achtergelaten;
- g: bij vertrek van de praktijk wordt gecontroleerd of er nog collega's in het pand aanwezig zijn. De laatst aanwezige zorgt ervoor dat alle ramen en deuren zijn gesloten;
- h: toegang tot het pand is alleen mogelijk met de sleutels in bezit van Daphne Meijer, andere huurders en de verhuurders. Sleutels worden niet aan derden afgegeven;

Daphne Meijer ziet op naleving van de hiervoor genoemde maatregelen.

Verwerkers

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

5. Informatieplicht

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

6. Verwerkingsregister

Daphne Meijer 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

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

Daphne Meijer maakt gebruik van de volgende verwerkers: PoZoB, PCD, E Health Minddistrict en Embloom.

Ontvangers

Daphne Meijer verstrekt persoonsgegevens van betrokkenen aan derden wanneer dat noodzakelijk is in het kader van de uitvoering van de behandelovereenkomst, of in geval van een wettelijke verplichting. Daarbuiten worden geen persoonsgegevens aan derden verstrekt zonder voorafgaande uitdrukkelijke toestemming van de betrokkene.

8. Bewaartermijnen

Daphne Meijer 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.

Daphne Meijer hanteert in beginsel de volgende bewaartermijnen:

- a. medische gegevens: ten minste 20 jaar na het einde van de behandelovereenkomst;
- b. (financieel-)administratieve gegevens: 7 jaar na vastlegging van de gegevens;
- c. gegevens van zzp'ers, anders dan (financieel-)administratieve gegevens: 5 jaar na het einde van de overeenkomst van opdracht;

9. Voorsnog geen gegevensbeschermingseffectbeoordeling (DPIA)

In uitzonderingsgevallen zou sprake kunnen zijn van het uitvoeren van een DPIA. In dat geval voert Daphne Meijer 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

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

Daphne Meijer heeft geen FG aangesteld aangezien **geen** sprake is van een grootschalige verwerking van bijzondere persoonsgegevens.

12. Beveiligingsincidenten

Daphne Meijer 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 Daphne Meijer 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.

Daphne Meijer documenteert alle inbreuken in verband met persoonsgegevens in het datalekkenregister.

Voor het geval dat een (potentieel) incident waarvan een door Daphne Meijer ingeschakelde verwerker eerder op de hoogte is geraakt, is in de verwerkersovereenkomst bepaald dat de verwerker Daphne Meijer 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. Daphne Meijer 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 Daphne Meijer, praktijk eigenaar, gz-psycholoog afgewikkeld.

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

Na ontvangst van een verzoek zal Daphne Meijer 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 Daphne Meijer 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 Daphne Meijer de verzoeker binnen de eerste maand.

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