

INTERN PRIVACYBELEID Praktijk Kom in je Kracht

1. Inleiding

Dit is het privacybeleid van Praktijk Kom in je Kracht. Dit privacybeleid heeft betrekking op het verwerken van (bijzondere) persoonsgegevens in het kader van zowel de zorgverlening als de (interne) bedrijfsvoering van Praktijk Kom in je Kracht.

Praktijk Kom in je Kracht is als zorgaanbieder verwerkingsverantwoordelijke. Praktijk Kom in je Kracht bepaalt het doel en de middelen voor de verwerking van (bijzondere) persoonsgegevens. Dit document beschrijft de wijze waarop Praktijk Kom in je Kracht 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. Vooralnog 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 Kom in je Kracht is in overeenstemming 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 Praktijk Kom in je Kracht daadwerkelijk wordt nageleefd.

3. Categorieën persoonsgegevens en verwerkingsdoelen

Praktijk Kom in je Kracht verwerkt persoonsgegevens van de volgende categorieën personen:

- a. (potentiële) patiënten;
- b. bezoekers aan het praktijkpand van Praktijk Kom in je Kracht;
- c. bezoekers van www.praktijkkominjekracht.nl;
- d. deelnemers aan bijeenkomsten van Praktijk Kom in je Kracht;
- e. alle overige personen die met Praktijk Kom in je Kracht contact opnemen of van wie Praktijk Kom in je Kracht persoonsgegevens verwerkt.

a. (potentiële) patiënten

Praktijk Kom in je Kracht 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 (Praktijkdata) van Praktijk Kom in je Kracht opgeslagen.

b. bezoekers aan de praktijk van Praktijk Kom in je Kracht

Registratie van aanwezigheid van een patiënt wordt in het ICT-systeem (Praktijkdata) van Praktijk Kom in je Kracht opgeslagen.

c. bezoekers van www.praktijkkominjekracht.nl

De website www.PraktijkKominjeKracht.nl verzamelt geen persoonsgegevens over bezoekers.

d. deelnemers aan bijeenkomsten van Praktijk Kom in je Kracht

Momenteel niet van toepassing. Indien wel van toepassing wordt intern privacybeleid gereviseerd.

e. overige personen

In het kader van de behandeling, kan Praktijk Kom in je Kracht ook gebruikmaken van gegevens afkomstig van andere hulpverleners.

4. Organisatorische en technische maatregelen / beveiliging

Uitgangspunt voor Praktijk Kom in je Kracht 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 Praktijk Kom in je Kracht passende technische en organisatorische maatregelen getroffen om persoonsgegevens te beschermen tegen verlies of onrechtmatige verwerking.

Interne maatregelen

Praktijk Kom in je Kracht heeft de volgende interne technische en organisatorische maatregelen getroffen:

- a. het uitwisselen van vertrouwelijke informatie met andere zorgverleners vindt (conform NEN 7510, NEN 7512 en NEN 7513) uitsluitend via een beveiligde verbinding (versleuteld mailverkeer via ZIVVER) plaats. 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 wordt uitsluitend opgeslagen in het ICT-systeem (Praktijkdata) 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. medewerker draagt ervoor zorg dat haar wachtwoord voor het ICT-systeem (Praktijkdata) van de praktijk voldoende sterk is en periodiek wordt gewijzigd, tevens wordt 2-staps-authenticatie toegepast;
- d. het is niet toegestaan apparatuur als laptops, tablets en mobiele telefoons onbeheerd buiten de praktijk achter te laten. Toegang tot dergelijke apparatuur is afgeschermd met een wachtwoord;
- e. inloggegevens worden vertrouwelijk behandeld en worden niet met derden gedeeld;
- f. bij (dagelijks) vertrek van de praktijk logt medewerker haar desktop computer volledig uit, sluit af en bergt eventuele papieren dossiers volledig en veilig op;
- g. het is niet toegestaan, zonder toestemming van Praktijk Kom in je Kracht, 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) is voorzien van actieve wachtwoordbeveiliging, firewall en virusscanner. Veiligheidsupdates worden tijdig uitgevoerd. Er wordt geen verbinding 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 schijf) met vertrouwelijke informatie onbeheerd in een auto of elders buiten de praktijk achter te laten;
- i. bij vertrek van de praktijk zorgt medewerker ervoor dat alle ramen en deuren zijn gesloten;
- j. toegang tot het pand is alleen mogelijk met aan medewerker verstrekte sleutels. Sleutels mogen niet aan derden worden afgegeven;

Praktijk Kom in je Kracht ziet toe op naleving van de hiervoor genoemde maatregelen.

Verwerkers

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

5. Informatieplicht

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

6. Verwerkingsregister

Praktijk Kom in je Kracht 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

Praktijk Kom in je Kracht kan bij het verwerken van persoonsgegevens gebruikmaken van externe dienstverleners. Deze dienstverleners verwerken uitsluitend persoonsgegevens op instructie van Praktijk Kom in je Kracht. Met deze partijen heeft Praktijk Kom in je Kracht 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.

Praktijk Kom in je Kracht maakt gebruik van de volgende verwerkers:

Praktijkdata – ECD
ZIVVER - mailsysteem

Ontvangers

Praktijk Kom in je Kracht 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

Praktijk Kom in je Kracht 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.

Praktijk Kom in je Kracht 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. 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. Voorsnog geen gegevensbeschermingseffectbeoordeling (DPIA)

In uitzonderingsgevallen zou sprake kunnen zijn van het uitvoeren van een DPIA. In dat geval voert Praktijk Kom in je Kracht 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

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

Praktijk Kom in je Kracht heeft geen FG aangesteld aangezien **geen** sprake is van een grootschalige verwerking van bijzondere persoonsgegevens (zie handleiding).

12. Beveiligingsincidenten

Praktijk Kom in je Kracht 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 Praktijk Kom in je Kracht 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 (Autoriteit Persoonsgegevens) 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.

Praktijk Kom in je Kracht documenteert alle inbreuken in verband met persoonsgegevens in het datalekkenregister.

Voor het geval dat een (potentieel) incident waarvan een door Praktijk Kom in je Kracht ingeschakelde verwerker eerder op de hoogte is geraakt, is in de verwerkersovereenkomst bepaald dat de verwerker Praktijk Kom in je Kracht 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. Praktijk Kom in je Kracht 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 Marjolein Raaijmakers, Praktijkhouder/GZ-psycholoog/Psychotherapeut, afgewikkeld.

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

Na ontvangst van een verzoek zal Praktijk Kom in je Kracht 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 Praktijk Kom in je Kracht 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 Praktijk Kom in je Kracht de verzoeker binnen de eerste maand.

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