

INTERN PRIVACYBELEID

J.S.T. Visser praktijk Cliënt Centraal Utrecht

1. Inleiding

Dit privacybeleid heeft betrekking op het verwerken van (bijzondere) persoonsgegevens in het kader van zowel de zorgverlening als de (interne) bedrijfsvoering van J.S.T. Visser

J.S.T. Visser is als zorgaanbieder verwerking verantwoordelijke en bepaalt het doel en de middelen voor de verwerking van (bijzondere) persoonsgegevens. Dit document beschrijft de wijze waarop J.S.T. Visser als verantwoordelijke 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. Doorgifte buiten de EU;
10. Geen functionaris voor de gegevensbescherming;
11. Beveiligingsincidenten;
12. Rechten van betrokkenen.

2. Actualisatie en controle naleving privacybeleid

De verwerking van persoonsgegevens binnen Psychotherapiepraktijk Cliënt Centraal Utrecht 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.

3. Categorieën persoonsgegevens en verwerkingsdoelen

Cliënt Centraal Utrecht verwerkt persoonsgegevens van de volgende categorieën personen:

- a. (potentiële) patiënten;
- b. bezoekers aan het praktijkpand
- c. bezoekers van www.cliëntcentraalutrecht.nl
- d. deelnemers aan bijeenkomsten van J.S.T Visser
- e. alle overige personen die contact opnemen of van wie J.S.T Visser persoonsgegevens verwerkt.

a. (potentiële) patiënten

Cliënt Centraal Utrecht 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 Cliënt Centraal Utrecht opgeslagen.

- b. deelnemers aan van bijeenkomsten

Tijdens intervisie bijeenkomsten, supervisie bijeenkomsten of andere bijeenkomsten van de praktijk kunnen persoonsgegevens worden genoteerd ten behoeve van doeleinden in het kader van accreditatie en visitatie.

c. overige personen

In het kader van de behandeling, kan Cliënt Centraal Utrecht ook gebruikmaken van gegevens afkomstig van andere hulpverleners.

4. Organisatorische en technische maatregelen / beveiliging

Uitgangspunt van Cliënt Centraal Utrecht 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 passende J.S.T. Visser technische en organisatorische maatregelen getroffen om persoonsgegevens te beschermen tegen verlies of onrechtmatige verwerking.

Interne maatregelen

Cliënt Centraal Utrecht hanteert interne technische en organisatorische maatregelen

- a. het uitwisselen van vertrouwelijke informatie met andere zorgverleners dient (conform NEN 7510, NEN 7512 en NEN 7513) uitsluitend via een beveiligde verbinding en versleuteld mailverkeer (ZorgMail is een beveiligd communicatiesysteem voor de zorgsector waarop Cliënt Centraal Utrecht is aangesloten). 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. het is niet toegestaan apparatuur als laptop, en mobiele telefoons onbeheerd buiten de praktijk achter te laten. Toegang tot dergelijke apparatuur dient te zijn 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 dient de medewerker zijn/haar desktop computer volledig uit te loggen, af te sluiten en eventuele papieren dossiers volledig en veilig op te bergen;
- f. 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 schijf) met vertrouwelijke informatie onbeheerd in een auto of elders buiten de praktijk achter te laten;

Verwerkers

Met verwerkers heeft Cliënt Centraal Utrecht 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.

5. Verwerkingsregister

Cliënt Centraal Utrecht 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.

6. Verwerkers en ontvangers

Cliënt Centraal Utrecht kan bij het verwerken van persoonsgegevens gebruikmaken van externe dienstverleners. Deze dienstverleners verwerken uitsluitend persoonsgegevens op instructie van J.S.T. Visser. Met deze partijen heeft J.S.T. Visser 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, privacy rechten van betrokkenen, audits en controle alsook het retourneren en/of verwijderen van persoonsgegevens door de verwerker.

Cliënt Centraal Utrecht maakt gebruik van de volgende verwerkers:

- | | |
|----------|--|
| AXIANS | - Online DBC een online portaal uitsluitend bedoeld voor geautoriseerde zorgprofessionals waar verwijzingen en gegevens kunnen worden uitgewisseld en met ene koppeling naar |
| ZorgMail | - Beveiligd communicatiesysteem voor de zorgsector, via e-mail en andere kanalen |

Ontvangers

Cliënt Centraal Utrecht 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.

7. Bewaartermijnen

Client Centraal Utrecht 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.

Cliënt Centraal Utrecht hanteert in beginsel de volgende bewaartermijnen:

- medische gegevens: ten minste 20 jaar na het einde van de behandelovereenkomst;
- (financieel-)administratieve gegevens: 7 jaar na vastlegging van de gegevens;

8. Doorgifte buiten EER

Cliënt Centraal Utrecht geeft in beginsel geen persoonsgegevens door aan landen buiten de Europese Economische Ruimte (EER). Indien dit toch noodzakelijk mocht zijn, draagt J.S.T. Visser 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.

9. 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.

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

10. Beveiligingsincidenten

Cliënt Centraal Utrecht 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 J.S.T. Visser 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.

Cliënt Centraal Utrecht documenteert alle inbreuken in verband met persoonsgegevens in het datalekken register.

Voor het geval dat een (potentieel) incident waarvan een door de praktijk ingeschakelde verwerker eerder op de hoogte is geraakt, is in de verwerkersovereenkomst bepaald dat de verwerker J.S.T. Visser 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 gegevens uitwissing, 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.

Verzoeken van betrokkenen met betrekking tot persoonsgegevens worden door J.S.T.Visser (psychotherapeut, klinisch psycholoog en eigenaar praktijk) afgewikkeld.

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

Na ontvangst van een verzoek zal J.S.T. Visser 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 J.S.T. Visser 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.

J.S.T. Visser stelt vast welk recht de verzoeker inroept en verzamelt in dat kader de benodigde gegevens, en 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.

Datum	oorsprong inbreuk	soort gegevens	aantal betrokkene	Risico's	Maatregelen	AP? (ja/n)	klanten? (ja/n)	afgehandeld door
						Nee (geen)	Nee	AB

14 Schema (boven) voor vastleggen van ongewone web activiteit (datalek), tot op heden hebben zich nog geen incidenten voorgedaan