**INTERN PRIVACYBELEID Mariëlle Schnitzeler (Bijlage B mei 2018)**

1. **Inleiding**

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

Mariëlle Schnitzeler is als zorgaanbieder verwerkingsverantwoordelijke. Mariëlle Schnitzeler bepaalt het doel en de middelen voor de verwerking van (bijzondere) persoonsgegevens. Dit document beschrijft de wijze waarop Mariëlle Schnitzeler 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 privacybeleid;
2. Categorieën persoonsgegevens en doelen;
3. Organisatorische en technische maatregelen / beveiliging;
4. Informatieplicht;
5. Verwerkingsregister;
6. Verwerkers en ontvangers;
7. Bewaartermijnen;
8. Vooralsnog geen gegevensbeschermingseffectbeoordeling (DPIA);
9. Doorgifte buiten de EU;
10. Geen functionaris voor de gegevensbescherming;
11. Beveiligingsincidenten;
12. Rechten van betrokkenen.
13. **Actualisatie en controle naleving privacybeleid**

De verwerking van persoonsgegevens binnen Praktijk Mariëlle Schnitzeler 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 verwerkers van Praktijk Mariëlle Schnitzeler daadwerkelijk wordt nageleefd.

1. **Categorieën persoonsgegevens en verwerkingsdoelen**

Mariëlle Schnitzeler verwerkt persoonsgegevens van de volgende categorieën personen

1. (potentiële) patiënten

Mariëlle Schnitzeler 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.

1. bezoekers van www.praktijkmarielleschnitzeler.com die belangstelling tonen voor behandeling of coaching.

De opgenomen gegevens van een patiënt worden in het papieren dossier van Mariëlle Schnitzeler opgeslagen en bewaard.

1. vertrouwelijke informatie mag alleen worden opgeslagen in het ICT-systeem van de praktijk als 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;
2. 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;
3. 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;
4. bij (dagelijks) vertrek van de praktijk dient Mariëlle Schnitzeler haar desktop computer volledig uit te loggen, af te sluiten en papieren dossiers volledig en veilig op te bergen;

*Verwerkers*

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

1. **Informatieplicht**

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

1. **Verwerkingsregister**

Mariëlle Schnitzeler 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.

1. **Verwerkers en ontvangers**

Verwerkers

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

Mariëlle Schnitzeler maakt gebruik van de volgende verwerkers:

Boshuis Belastingadvies in de persoon van Frederike Boshuis.

Ontvangers

Mariëlle Schnitzeler 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.

1. **Bewaartermijnen**

Mariëlle Schnitzeler 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.

Mariëlle Schnitzeler hanteert in beginsel de volgende bewaartermijnen:

1. medische gegevens: ten minste 15 jaar na het einde van de behandelovereenkomst;
2. (financieel-)administratieve gegevens: 7 jaar na vastlegging van de gegevens;
3. **Vooralsnog geen gegevensbeschermingseffectbeoordeling (DPIA)**

In uitzonderingsgevallen zou sprake kunnen zijn van het uitvoeren van een DPIA. In dat geval voert Mariëlle Schnitzeler 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.

1. **Doorgifte buiten EER**

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

1. **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.

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

1. **Beveiligingsincidenten**

Mariëlle Schnitzeler 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 Mariëlle Schnitzeler 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.

Mariëlle Schnitzeler documenteert alle inbreuken in verband met persoonsgegevens in het datalekkenregister.

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

1. **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. Mariëlle Schnitzeler 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 Mariëlle Schnitzeler, praktijkhouder Praktijk Mariëlle Schnitzeler, afgewikkeld.

Na ontvangst van een verzoek zal Mariëlle Schnitzeler 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 Mariëlle Schnitzeler 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 Mariëlle Schnitzeler de verzoeker binnen de eerste maand.

Mariëlle Schnitzeler stelt vast welk recht de verzoeker inroept en verzamelt in dat kader de benodigde gegevens. Mariëlle Schnitzeler 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.

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. Mariëlle Schnitzeler stelt vast of daarvan sprake is en noteert de derde partijen in zijn verslag. Dergelijke kennisgevingen aan externe partijen laat Mariëlle Schnitzeler achterwege als dit onmogelijk blijkt of onevenredig veel inspanning vergt.