Reglement AVG- Privacybeleid **Praktijk Osteopathie Culemborg (POC)** - Privacystatement

De **Autoriteit Persoonsgegevens** (hierna **AP**) controleert of organisaties zich aan de wetgeving houden. Ter voorbereiding op deze regelgeving heeft de AP een stappenplan opgesteld:

Het AVG-10 stappenplan:
1) Bewustwording
2) Rechten van betrokkenen
3) Overzicht verwerkingen
4) Data protection impact assessment (DPIA)
5) Privacy by design & privacy by default
6) Functionaris voor de gegevensbescherming
7) Meldplicht datalekken
8) Verwerkersovereenkomsten
9) Leidende toezichthouder
10) Toestemming

Een nadere uitwerking van dit stappenplan en naleving in de praktijk daarvan dient ervoor zorg te dragen dat **POC** zich zoveel mogelijk aan de wetgeving AVG kan houden. Hieronder zullen de verschillende stappen worden besproken. Daarbij wordt nagegaan in hoeverre deze punten binnen **POC** gelden, waar **POC** tegen aan loopt en op welke wijze **POC** op een verantwoorde manier aan de 'nieuwe' verplichtingen kan voldoen.

1 Bewustwording

1. **POC** is een praktijk waarbinnen **Arjen Volkers en Mascha Vogel** osteopathie als dienstverlening aanbieden. Om dat doel te kunnen uitvoeren dient **POC** persoonsgegevens van patiënten te verwerken en gebruiken binnen de dagelijkse bedrijfsvoering.

2. De gegevens die worden gedocumenteerd zijn privacygevoelig. Het gaat om persoonsgegevens, aan de hand waarvan de betrokkene zowel direct als indirect geïdentificeerd kan worden. Om er zeker van te zijn dat er op een verantwoorde wijze met deze gegevens wordt omgegaan en dat de praktijk voldoet aan de privacywetgeving, heeft **POC** bovengenoemde AVG-stappenplan doorlopen.

3. Het betreft hier registratie van persoonsgegevens met een gerechtvaardigd belang. Immers de patiënten melden zichzelf aan bij **POC**. Zij willen graag geholpen worden door de osteopaat voor hun klachten.

2. Rechten van betrokkenen

2.1 Om een eerlijke verwerking van persoonsgegevens te waarborgen geeft de Verordening diverse rechten aan de betrokkene. De betrokkene kan deze rechten uitoefenen tegen de verwerkingsverantwoordelijke. De betrokkene heeft:
- het recht op informatie over de verwerkingen;
- het recht op inzage in zijn gegevens;
- het recht op correctie van de gegevens als deze niet kloppen;
- het recht op verwijdering van de gegevens en 'het recht om vergeten te worden';
- het recht op beperking van de gegevensverwerking;
- het recht op verzet tegen de gegevensverwerking;
- het recht op overdracht van zijn gegevens (dataportabiliteit);

• het recht om niet onderworpen te worden aan een geautomatiseerde besluitvorming.

2.2 Een patiënt of voormalig patiënt (de betrokkene) kan om bovenstaande gegevens verzoeken. De betrokkene kan zulks doen per mail naar **arjenvolkers@osteopathieculemborg.nl** of **maschavogel@osteopathieculemborg.nl**.
De betrokkene dient zich daarbij te legitimeren, opdat **POC** met voldoende zekerheid kan vaststellen dat degene die het verzoek doet daadwerkelijk de betrokkene is.

2.3 **POC** zal binnen 1 maand na ontvangst van het verzoek betrokken informeren over de uitvoering van het verzoek. Bij complexe, of een veelvoud aan verzoeken kan deze termijn verlengd worden met maximaal 2 maanden. De betrokkene zal in een dergelijk geval van verlengde termijn van uitvoering van het verzoek daaromtrent geïnformeerd worden. De informatie wordt in principe schriftelijk verstrekt.

2.4 In sommige gevallen mag **POC** weigeren tot uitvoering van het verzoek om gegevensverstrekking over te gaan, dan wel daarvoor kosten in rekening brengen. Het moet dan gaan om de situatie dat de betrokkene buitensporige of ongegronde verzoeken doet. (Bijvoorbeeld meerdere verzoeken achter elkaar om dezelfde gegevens. Dan wel wanneer sprake is van een van de beschermende noodzakelijkheidscriteria welke de AVG kent zoals bijvoorbeeld in het kader van een (strafrechtelijk) onderzoek naar de betrokkene). Indien **POC** weigert aan het verzoek te voldoen, zal **POC** zulks motiveren en de betrokkene wijzen op het klachtrecht bij de toezichthouder AVG.

2.5 **POC** realiseert zich dat indien zij een schriftelijke beslissing neemt in het kader van de uitoefening van de rechten van de betrokkene, dat dit dan geldt als een besluit in de zin van de Algemene wet bestuursrecht.

2.6 In sommige gevallen dient **POC** de betrokken patiënt uit zichzelf te informeren. Dit is het geval indien:
- gegevens buiten de betrokkene om worden verkregen
- gegevens voor een ander doel gebruikt gaan worden dan waar de gegevens oorspronkelijk voor waren afgegeven. **POC** zal in die gevallen binnen 1 maand betrokkene informeren.

2.7 Indien de behandeling van de patiënt eindigt zal **POC** de persoonsgegevens nog enige tijd in haar systeem bewaren. De wet Wgbo bepaalt dat medische dossiers 20 jaar moeten worden bewaard. Aan die bewaartermijn zal **POC** zich houden. De dossiers zullen **na 20 jaar** vernietigd worden. Binnen het dossier bevinden zich tevens gegevens van niet medische aard.

2.8 Ten einde er zeker van te zijn dat de betrokkene een volledig beeld heeft van de wijze waarop met diens persoonsgegevens wordt omgegaan en met welk doel en onder welke grondslag (gerechtvaardigd belang), zal iedere betrokken bij registratie toegang krijgen tot deze privacystatement en de hierbij behorende documenten. **POC** zal deze gegevens op de website plaatsen en iedere betrokkene op die vindplaats wijzen.

3. Register van verwerkingsactiviteiten

1. **POC** verwerkt persoonsgegevens van patiënten. Ten aanzien van al deze vormen van verwerkingen van persoonsgegevens zal **POC** een register van verwerkingsactiviteiten bijhouden. Daarin worden alle soorten persoonsgegevens die verwerkt zullen worden opgenoemd.

2. In het geval de patiënt een klacht indient tegen de osteopaat, zullen die gegevens eveneens worden verwerkt door **POC**.

4 DPIA (Data protection impact assessment)

4.1 DPIA staat voor gegevensbeschermingseffectbeoordeling. Een DPIA is alleen verplicht wanneer sprake is van gegevensverwerking welke waarschijnlijk een hoog privacyrisico oplevert. Binnen de AVG worden drie situaties besproken wanneer sprake is van verhoogd risico:

- systematisch en uitvoerig persoonlijke aspecten evalueren
- op grote schaal bijzondere persoonsgegevens verwerken
- op grote schaal en systematisch mensen volgen in een publiek toegankelijk gebied

4.2 Naast de criteria uit de AVG zelf heeft de werkgroep van Europese privacytoezichthouders een lijst met 9 criteria opgesteld om nader te bezien of een DPIA nodig is. De criteria die op osteopaten van toepassing zouden kunnen zijn:

- gevoelige gegevensverwerking
- grootschalige gegevensverwerking
- gegevensverwerking over kwetsbare personen

4.3 De privacytoezichthouders zien verwerkingen van bijzondere persoonsgegevens door individuele artsen niet als grootschalig. Individuele artsen hoeven dus geen DPIA uit te voeren. Het ligt voor de hand dat de gegevensverwerking door de individuele osteopaat aldus evenmin de uitvoering van een DPIA behoeft. **POC** zal zodoende geen DPIA uitvoeren.

4.4 Evenwel is **POC** zich ervan bewust dat sprake is van bijzondere persoonsgegevens. De inhoud van een medisch dossier is gevoelig voor de betrokkene en vergt een grote mate van vertrouwelijkheid. **POC** zal zich zodoende inzetten die gegevens vertrouwelijk te laten blijven.

4.5 De gegevens zoals **POC** registreert zijn slechts bedoeld voor intern gebruik. De persoonsgegevens worden gebruikt om te waarborgen dat de osteopaat de patiënt zo goed mogelijk van dienst kan zijn. Van dienst zijn in het verhelpen van de klachten en van dienst zijn door het mogelijk maken dat de ziektekostenverzekering de kosten zoveel mogelijk vergoedt.

4.6 Op termijn zal de Autoriteit Persoonsgegevens (AP) een lijst van verwerkingen publiceren waar een DPIA voor verplicht is. Zodra die lijst er is, zal **POC** haar verwerking van persoonsgegevens opnieuw tegen het licht houden om te bezien of nog nadere maatregelen nodig zijn.

5. Privacy by design & privacy by default

5.1. Privacy door ontwerp en door standaardinstellingen voor producenten. **POC** is producent van een dienst, welke wordt ondersteund door de verwerking van persoonsgegevens. Zodoende houdt **POC** bij de ontwikkeling en uitwerking van die dienst rekening met het recht op bescherming van persoonsgegevens. Met inachtneming van de stand van de techniek ziet **POC** erop toe dat de verwerkingsverantwoordelijken en de verwerkers in staat zijn te voldoen aan hun verplichtingen inzake gegevensbescherming.

5.2. **POC** let daarbij op:

- het minimaliseren van de verwerking van persoonsgegevens;
- slechts het BSN-nummer noteren, doch geen kopie maken van de het paspoort/ID kaart;
- transparantie met betrekking tot de functies en de verwerking van persoonsgegevens;
- het in staat stellen van de betrokkene om controle uit te oefenen op de informatieverwerking; en
- beveiligingskenmerken creëren en verbeteren.

6. Functionaris voor de gegevens bescherming

6.1. Net als voor de DPIA geldt dat de individuele praktijk van een osteopaat door de AP niet wordt gezien als een grootschalige verwerker. Het instellen van een FG is ondanks dat het gaat om bijzondere persoonsgegevens niet noodzakelijk. Daarbij stipt **POC** nogmaals aan dat in deze sprake is van het verwerken van persoonsgegevens op verzoek van de patiënt, nu deze een zo goed mogelijke behandeling wenst. **POC** verwerkt geen persoonsgegevens voor commerciële doeleinden. Patiënten worden niet gevolgd door **POC** aan de hand van de persoonsgegevens.

6.2. **POC** benadrukt opnieuw zich te realiseren persoonsgegevens te verwerken die een hoge mate van vertrouwelijkheid kennen. **POC** meent echter alle maatregelen te hebben genomen, ten einde erop toe te zien dat de persoonsgegevens van patiënten niet voor andere doeleinden gebruikt worden dan bedoeld is.

7. Meldplicht Datalekken

7.1. Een datalek in de zin van de AVG is een inbreuk in verband met persoonsgegevens. Het is een inbreuk op de beveiliging die leidt tot de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.

7.2. Het is voor de kwalificatie als ‘inbreuk in verband met persoonsgegevens’ niet relevant dat er boze opzet in het spel is. Naast het ‘hacken’ van persoonsgegevens, kan ook gedacht worden aan gegevens die op een verloren laptop staan of een afgesloten website met persoonsgegevens die per ongeluk openstaat. Een inbreuk op de beveiliging houdt in dat zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Er is niet uitsluitend sprake van een dreiging, of van een tekortkoming in de beveiliging (ook wel aangeduid als een beveiligingslek) die zou kunnen leiden tot een beveiligingsincident. Er heeft zich daadwerkelijk een beveiligingsincident voorgedaan, waarbij de getroffen preventieve maatregelen niet toereikend waren om dit te voorkomen.

7.3. **POC** zal ieder datalek aan de AP melden, tenzij onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. **POC** zal binnen 72 uur na ontdekking de AP in kennis stellen, ook indien nog niet alle informatie voorhanden is.

7.4. Bovendien zal **POC** het datalek onverwijld melden aan de betrokkenen, indien sprake is van een hoog risico door de inbreuk op de persoonsgegevens. Voor de vraag of sprake is van een hoog risico zal **POC** eerst nader onderzoek daarnaar mogen doen.

7.5. Het datalek zal door **POC** gedocumenteerd worden in een overzicht van datalekken die zich binnen **POC** hebben voorgedaan. Niet alleen zullen de feiten omtrent de inbreuk en de gevolgen daarvan in dit overzicht worden gedocumenteerd, doch eveneens de genomen corrigerende maatregelen.

8. Verwerkersovereenkomsten

8.1. **POC** maakt gebruik van het bedrijf **crossuite** voor het verwerken van de persoonsgegevens in een patiëntenbeheerplatform. Dit bedrijf dient zodoende gezien te worden als een verwerker. Ten einde ervan verzekerd te zijn dat **crossuite** zich aan de vereisten houdt welke nodig zijn om te voldoen aan de AVG heeft **POC** een verwerkersovereenkomst afgesloten met **crossuite**.

8.2. Binnen de verwerkersovereenkomst met **crossuite** zijn in ieder geval de volgende zaken geregeld:

- het onderwerp en de duur van de verwerking;
- de aard en het doel van de verwerking;
- het soort persoonsgegevens en de categorieën van betrokkenen;
- de rechten en verplichtingen van de verwerkingsverantwoordelijke.
- de persoonsgegevens alleen verwerkt worden onder schriftelijke instructie van **POC**, onder andere voor wat betreft de doorgifte van persoonsgegevens aan een derde land of een internationale organisatie (tenzij deze daartoe wettelijk is verplicht);
- waarborg van de verwerker dat de toegang tot die gegevens is beperkt tot gemachtigde personen. Deze personen moeten gebonden zijn aan geheimhouding op grond van een overeenkomst of een wettelijke verplichting;
- de verwerker minimaal hetzelfde niveau van beveiliging van de persoonsgegevens hanteert als **POC** doet;
- de verwerker zal **POC** alle mogelijke ondersteuning bieden bij het nakomen van haar verplichtingen met het oog op beantwoording van verzoeken rondom de rechten van betrokkenen;
- verwerker **POC** zal bijstaan bij het nakomen van haar verplichtingen op het gebied van beveiliging van persoonsgegevens en de meldplicht datalekken;
- na beëindiging van de overeenkomst tussen **POC** en verwerker, de in uw opdracht verwerkte persoonsgegevens wist of aan **POC** teruggeeft, en bestaande kopieën verwijdert;
- **POC** alle informatie ter beschikking stelt die nodig is om aantoonbaar te maken dat de verplichtingen op grond van de Verordening rondom het inzetten van een verwerker worden nageleefd en die nodig is om audits mogelijk te maken;
- verwerker maakt inzichtelijk welke afspraken deze met betrekking tot sub-verwerkers maakt;
- verwerker vermeldt de goedgekeurde gedragscodes en certificeringsmechanismen waar verwerker bij diens werkzaamheden gebruik van maakt;
- verwerker garandeert **POC** aan alle verplichtingen te voldoen zoals de AVG van verwerker verlangt.

8.3 **POC** maakt geen gebruik van andere verwerkers dan **crossuite**. Wel maakt **POC** gebruik van een boekhouder. Deze verwerkte geen gegevens van patiënten, maar

heeft wel inzage in sommige persoonsgegevens. Vooral de gegevens rondom betalingen zal de boekhouder in kunnen zien. Zodoende heeft boekhouder een geheimhoudingsverklaring ondertekend. In die verklaring wordt niet alleen weergegeven dat de boekhouder zelf geheimhouding zal betrachten over alle persoonsgegevens die deze te zien krijgt van patiënten van **POC**, ook de medewerkers en derden waar de boekhouder gebruik van maakt hebben diezelfde geheimhoudingsplicht. Bovendien is in de verklaring opgenomen dat de boekhouder geen persoonsgegevens van patiënten zal verwerken.

9. Leidende Toezichthouder

9.1. **POC** dient te bepalen onder welke toezichthouder zij valt. **POC** heeft 1 vestiging te **Culemborg**. Dit is op Nederlandse bodem. De werkzaamheden van **POC** rusten op Nederlands grondgebied. De Leidende toezichthouder voor **POC** is dus de Autoriteit Persoonsgegevens te Nederland.

10. Toestemming

10.1. Voor de verwerking van bepaalde gegevens is toestemming nodig van de betrokkene. Dat is het geval indien het gaat om bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard. Ook het nationaal identificatienummer (BSN) is een zaak waarbij expliciete toestemming van de betrokkene nodig is, indien dat nummer wordt verwerkt. **POC** verwerkt het BSN-nummer van haar patiënten nu Osteopaten verplicht zijn dit nummer te gebruiken in correspondentie met andere zorgverleners. Het verwerken van gegevens over de gezondheid betreft eveneens een bijzondere categorie gegevens waarvan voor de verwerking toestemming nodig is van de patiënt. Het heeft echter de sterke voorkeur het verwerken van alle persoonsgegevens op voorhand met patiënten te bespreken en bij die verwerking expliciet te vermelden of de patiënt toestemming heeft gegeven voor die verwerking.

10.2. **POC** zal op de volgende wijze invulling geven aan deze benodigde toestemming. Naast het opstellen van een behandelplan zal bij de intake van een patiënt een overzicht worden gegeven van de afspraken. Deze zullen met de patiënt worden doorgenomen en vervolgens aan de patiënt ter hand worden gesteld dan wel aan de patiënt worden verzonden per mail, waarbij aangetekend wordt dat het hier een bevestiging van de gemaakte afspraken betreft. Er zal om een ontvangstbevestiging worden verzocht bij de patiënt. Op deze ‘opdrachtbevestiging’ zullen de belangrijkste gegevens worden benoemd over wat de patiënt kan verwachten van de osteopaat. Het gaat om het volgende:

- dat patiënt is gewezen op het feit dat persoonsgegevens verwerkt zullen worden en om welke persoonsgegevens het gaat;
- dat patiënt voor die verwerking expliciet toestemming heeft verleend;
- dat patiënt rechten heeft ten aanzien van het verwerken van persoonsgegevens en dat patiënt deze en de verdere werkwijze van **POC** met betrekking tot die persoonsgegevens kan nalezen in het onderhavige reglement zoals op de website van **POC** staat vermeld;
- dat patiënt gewezen wordt op de bewaartermijn(en) van de persoonsgegevens;

- dat patiënt de mogelijkheid heeft een klacht tegen **POC** in te dienen bij het NRO of NOF;
- wat het consulttarief is van **POC**.

11. Slotwoord

11.1 **POC** gaat ervan uit met dit privacybeleid aan alle vereisten van de nieuwe AVG-regels te voldoen. **POC** is zich ervan bewust dat sprake is van nieuwe regelgeving en dat zulks inhoudt dat nog niet alle facetten zich even makkelijk laten uiteenzetten. **POC** zal de aanpassingen, beslissingen en verder nieuws vanuit de AP volgen, opdat tijdige maatregelen genomen kunnen worden deze beleidsregels alsnog verder aan te scherpen, of bij te snijden.