Reglement AVG - Privacy Beleid Purus Osteopathie

Op 25 mei 2018 is nieuwe Privacywetgeving in werking getreden. Het gaat dan om Privacy Richtlijn (95/46/EG) en de Richtlijn Privacy en elektronische communicatie (2002/58/EG), de nationale wetten ter uitvoering van deze richtlijnen en/of, in voorkomend geval, de verordening (EU) 2016/679 (de "Algemene Verordening Gegevensbescherming"). Een en ander samengevat als de AVG. Deze wetgeving zal de wet Bescherming persoonsgegevens vervangen. De AVG verwacht een meer pro actieve rol van iedere organisatie die persoonsgegevens verwerkt. De meest relevante wijzigingen waar rekening mee dienen te worden gehouden zijn:

- versterking en uitbreiding van privacy rechten
- meer verantwoordelijkheden voor organisaties
- dezelfde, stevige bevoegdheden voor alle Europese privacy toezichthouders, zoals de bevoegdheid om boetes tot 20 miljoen euro op te leggen.

De Autoriteit Persoonsgegevens (hierna AP) blijft net als voorheen onder de wet Bescherming persoonsgegevens de autoriteit die controleert of organisaties zich aan de wetgeving houden.

Purus Osteopathie beschrijft hieronder hoe zij op een verantwoorde manier voldoet aan de wetgeving AVG.

1. Bewustwording

Purus Osteopathie is een praktijk waar osteopathie wordt beoefent. Om deze dienst te kunnen uitvoeren verwerkt Purus Osteopathie persoonsgegevens van cliënten en worden deze gegevens gebruikt binnen de dagelijkse bedrijfsvoering.

1.1. De gegevens die worden gedocumenteerd zijn privacy gevoelig. Het gaat om persoonsgegevens, aan de hand waarvan de betrokkene zowel direct als indirect geïdentificeerd kan worden. Ten einde er zeker van te zijn dat met die gegevens wordt omgegaan op een wijze die verantwoord is en voldoet aan de privacy wetgeving zoals per 25 mei 2018 van kracht zal worden heeft Purus Osteopathie ervoor gekozen met het onderhavige protocol in kaart te brengen, aan de hand van het AVG stappenplan (zoals hiervoor opgesomd),op welke wijze invulling gegeven dient te worden aan de AVG.

1.2. Het betreft hier registratie van persoonsgegevens met een gerechtvaardigd belang. De cliënten maken zelf een afspraak bij Purus Osteopathie, omdat ze graag geholpen willen worden bij hun hulpvraag.

2. Rechten van betrokken

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 (data portabiliteit)
- het recht om niet onderworpen te worden aan een geautomatiseerde besluitvorming.

2.2. Een client of voormalig client (de betrokkene) kan om bovenstaande gegevens verzoeken. De betrokkene kan zijn verzoek mailen naar info@purus-osteopathie.nl. De betrokkene dient zich daarbij te legitimeren, zodat Purus Osteopathie met voldoende zekerheid kan vaststellen dat degene die het verzoek doet daadwerkelijk de betrokkene is.

2.3. Purus Osteopathie zal binnen een maand, na ontvangst van het verzoek, de betrokkene informeren over de uitvoering van het verzoek. Bij complexe, of een veelvoud aan verzoeken kan dit termijn verlengd worden met maximaal twee maanden. De betrokkene zal daarover, via de mail, geïnformeerd worden.

2.4. In sommige gevallen mag Purus Osteopathie weigeren tot het uitvoeren van een gegevensverstrekking verzoek en kunnen er kosten in rekening gebracht worden. Het zal gaan om een buitensporig of ongegrond verzoek. U kunt denken aan:

- meerdere verzoeken achter elkaar om dezelfde gegevens
- als er 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 Purus Osteopathie uw verzoek weigert, zal Purus Osteopathie motiveren en de betrokkene wijzen op het klachtrecht bij de toezichthouder AVG.

2.5. Purus Osteopathie 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 Purus Osteopathie de betrokken client uit zichzelf te informeren. Dit is het geval indien:
- de gegevens buiten de betrokkene om zijn verkregen
- de gegevens voor een ander doel gebruikt gaan worden dan waar de gegevens oorspronkelijk voor waren afgegeven

Purus Osteopathie zal in die gevallen binnen een maand de betrokkene informeren.

2.7. Indien de behandeling van de client eindigt zal Purus Osteopathie persoonsgegevens nog enige tijd in haar systeem bewaren. De wet wgbo bepaalt dat medische dossiers 15 jaar moeten worden bewaard. Aan die bewaartermijn zal Purus Osteopathie zich houden. De dossiers zullen na 15 jaar vernietigd worden. Binnen het dossier bevinden zich ook 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 privacy statement en de hierbij behorende documenten. Purus Osteopathie zal deze gegevens op de website plaatsen.

3. Register van verwerkingsactiviteiten

3.1. Purus Osteopathie verwerkt persoonsgegevens van cliënten. Ten aanzien van al deze vormen van verwerkingen van persoonsgegevens zal Purus Osteopathie een register van verwerkingsactiviteiten bijhouden, in Crossuite.

3.2. In het geval dat de client een klacht indient tegen de osteopaat, zullen die gegevens eveneens worden verwerkt door Purus Osteopathie.

4. DPIA (Data protection impact assessment)

4.1. DPIA staat voor gegevens bescherming effect beoordeling. Een DPIA is alleen verplicht wanneer sprake is van gegevensverwerking wat een hoog privacy risico 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 privacy toezichthouders 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 gegevens verwerking
- grootschalige gegevens verwerking
- gegevensverwerking over kwetsbare personen

4.3. De privacy toezichthouders 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. Purus Osteopathie zal zodoende geen DPIA uitvoeren.

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

4.5. De gegevens zoals Purus Osteopathie registreert zijn bedoeld voor intern gebruik. De persoonsgegevens worden gebruikt om de client zo goed mogelijk van dienst te kunnen zijn. Dit houdt in:
- behandelen en verhelpen van de hulpvraag
- 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 Purus Osteopathie 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. Purus osteopathie is producent van een dienst, welke wordt ondersteund door de verwerking van persoonsgegevens. Zodoende houdt Purus Osteopathie de ontwikkeling en uitwerking van die dienst online schriftelijk bij, rekening houdend met het recht op bescherming van persoonsgegevens. Met inachtneming van de stand van de techniek ziet Purus Osteopathie erop toe dat de verwerkingsverantwoordelijken en de verwerkers in staat zijn te voldoen aan hun verplichtingen inzake gegevensbescherming.

5.2. Purus Osteopathie let daarbij op:
- het minimaliseren van de verwerking van persoonsgegevens
- slechts het BSN nummer noteren, doch geen kopie maken van 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
- 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 Purus Osteopathie aan dat in deze sprake is van het verwerken van persoonsgegevens op verzoek van de client, nu deze een zo goed mogelijke behandeling wenst. Purus Osteopathie verwerkt geen persoonsgegevens voor commerciële doeleinden. Cliënten worden niet gevolgd door Purus Osteopathie aan de hand van de persoonsgegevens.

6.2. Purus Osteopathie benadrukt opnieuw zich te realiseren persoonsgegevens te verwerken die een hoge mate van vertrouwelijkheid kennen. Purus Osteopathie meent echter alle maatregelen te hebben genomen, ten einde erop toe te zien dat de persoonsgegevens van cliënten 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. Purus Osteopathie zal ieder datalek aan de AP melden, tenzij onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Purus Osteopathie zal binnen tweeënzeventig uur na ontdekking de AP in kennis stellen, ook indien nog niet alle informatie voorhanden is.

7.4. Bovendien zal Purus Osteopathie 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 Purus Osteopathie eerst nader onderzoek daar naar mogen doen.

7.5. Het datalek zal door Purus Osteopathie gedocumenteerd worden in een overzicht van datalekken die zich binnen de praktijk 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. Purus Osteopathie maakt gebruik van het systeem Crossuite, voor het verwerken van de persoonsgegevens in een cliënten beheer platform. 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 Purus Osteopathie 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 Purus Osteopathie, 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 Purus Osteopathie
- de verwerker zal Purus Osteopathie alle mogelijke ondersteuning bieden bij het nakomen van haarverplichtingen met het oog op beantwoording van verzoeken rondom de rechten van betrokkenen
- verwerker Purus Osteopathie 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 Purus Osteopathie en verwerker, de in uw opdracht verwerkte persoonsgegevens wist of aan Purus Osteopathie teruggeeft, en bestaande kopieën verwijdert
- Purus Osteopathie 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 Purus Osteopathie aan alle verplichtingen te voldoen zoals de AVG van verwerker verlangt

8.3. Purus Osteopathie maakt geen gebruik van andere verwerkers dan Crossuite. Wel maakt Purus Osteopathie gebruik van een accountant. Deze verwerkte geen gegevens van cliënten, maar heeft wel inzage in sommige persoonsgegevens. Vooral de gegevens rondom betalingen zal de accountant in kunnen zien. Zodoende heeft een accountant een geheimhoudingsverklaring ondertekend. In die verklaring wordt niet alleen weergegeven dat de accountant zelf geheimhouding zal betrachten over alle persoonsgegevens die deze te zien krijgt van cliënten van Purus Osteopathie, ook de medewerkers en derden waar de accountant gebruik van maakt hebben diezelfde geheimhoudingsplicht. Bovendien is in de verklaring opgenomen dat de accountant geen persoonsgegevens van cliënten zal verwerken.

9. Leidende Toezichthouder

9.1. Purus Osteopathie dient te bepalen onder welke toezichthouder zij valt. Purus Osteopathie heeft 2 vestigingen te IJsselstein en Soest. De werkzaamheden van Purus Osteopathie rusten op Nederlands grondgebied. De Leidende toezichthouder voor Purus Osteopathie 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. Purus Osteopathie verwerkt het BSN nummer van haar cliënten omdat osteopaten verplicht zijn het BSN 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 client. Het heeft echter de sterke voorkeur het verwerken van alle persoonsgegevens op voorhand met cliënten te bespreken en bij die verwerking expliciet te vermelden of de client toestemming heeft gegeven voor die verwerking.

10.2. Purus Osteopathie zal op de volgende wijze invulling geven aan deze benodigde toestemming. De afspraken zullen mondeling met de client worden doorgenomen. Het gaat om het volgende:

- dat de client is gewezen op het feit dat persoonsgegevens verwerkt zullen worden en om welke persoonsgegevens het gaat
- dat de client voor die verwerking expliciet, mondeling, toestemming heeft verleend
- dat de client rechten heeft ten aanzien van het verwerken van persoonsgegevens en dat client deze en de verdere werkwijze van Purus Osteopathie met betrekking tot die persoonsgegevens kan nalezen in het onderhavige reglement zoals op de website van Purus Osteopathie staat vermeld
- dat de client de mogelijkheid heeft een klacht tegen Purus Osteopathie in te dienen bij het NRO of NVO
- wat het consulttarief is van Purus Osteopathie

In Crossuite wordt, door Purus Osteopathie in bijzijn van betrokkene, een vinkje voor akkoord geplaatst als dit besproken is.

11. Slotwoord

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