

Stap 3: Verwerkersovereenkomst

Bij 'Stap 1: Inventarisatie Persoonsgegevens' ben je nagegaan welke persoonsgegevens er binnen jouw organisatie (massagepraktijk) gebruikt worden. Bij 'Stap 2: Verwerkingsregister en Privacy Policy' heb je de inventarisatie uitgebreid met de grondslag, verwerking, bewaartermijn en beveiliging van de persoonsgegevens en heb je dit vastgelegd in een Verwerkingsregister. Ook heb je een Privacy Policy opgesteld. In deze derde stap, ontvang je ondersteuning voor het opstellen van verwerkersovereenkomsten.

Als organisatie (massagepraktijk) mag je persoonsgegevens niet doorgeven aan een andere partij zonder een verwerkersovereenkomst en zonder dat dit noodzakelijk is voor de doeleinden waarvoor je deze gegevens hebt verkregen (bijvoorbeeld het uitbesteden van de personeelsadministratie aan een administratiekantoor).

Wanneer is jouw organisatie (massagepraktijk) de 'verwerkingsverantwoordelijke'?

Wanneer de organisatie (massagepraktijk) zelf het doel en de middelen voor de verwerking van persoonsgegevens vaststelt, is de organisatie (massagepraktijk) verwerkingsverantwoordelijke.

Wanneer is jouw organisatie (massagepraktijk) een 'verwerker'?

Verwerkt de organisatie (massagepraktijk) in opdracht van een verantwoordelijke persoonsgegevens? Dan is de organisatie (massagepraktijk) de verwerker.

Let op! Ook als verwerker dien je een verwerkingsregister op te stellen en bij te houden (Zie Stap 2: Verwerkingsregister en Privacy Policy). Als verwerker van persoonsgegevens neem je de volgende informatie op in het verwerkingsregister:

- *De naam en contactgegevens van jouw organisatie (massagepraktijk), de vertegenwoordiger van jouw organisatie (massagepraktijk) of de verwerkingsverantwoordelijke;*
- *De naam en contactgegevens van de Functionaris voor de Gegevensbescherming (FG) als je die hebt aangesteld;*
- *Een beschrijving van de categorieën van verwerkingen die je in opdracht van iedere verantwoordelijke uitvoert;*
- *De naam en contactgegevens van eventuele andere (internationale) organisaties met wie je persoonsgegevens deelt;*
- *Een algemene beschrijving van de technische en organisatorische maatregelen die je hebt genomen om persoonsgegevens die je verwerkt te beveiligen.*

Verwerkersovereenkomst

In een verwerkersovereenkomst spreek je af wat de andere partij met de door jou verzamelde gegevens mag doen én vooral ook wat niet. Er worden afspraken vastgelegd met het oog op de naleving van de AVG, zoals over het doel van de verwerking en de beveiliging van gegevens. Met een verwerkersovereenkomst sluit je uit dat de andere partij de persoonsgegevens voor eigen doelen mag verwerken.

Je mag als verwerkingsverantwoordelijke alleen verwerkers inschakelen die voldoende garanties bieden dat zij aan de wettelijke vereisten voldoen.

Let op: als je de gegevensverwerking door een verwerker laat uitvoeren, dan ben je nog steeds verantwoordelijk voor de naleving van de Algemene verordening gegevensbescherming (AVG).

In de verwerkersovereenkomst moeten in ieder geval de volgende onderwerpen worden vastgelegd:

- Algemene beschrijving
Een omschrijving van het onderwerp, de duur, de aard en het doel van de verwerking, het soort persoonsgegevens, de categorieën van betrokkenen en jouw rechten en verplichtingen als verwerkingsverantwoordelijke (nu nog 'verantwoordelijke' genoemd).
- Instructies verwerking
De verwerking vindt in principe uitsluitend plaats op basis van jouw schriftelijke instructies. De verwerker mag de persoonsgegevens niet voor eigen doeleinden gebruiken.
- Geheimhoudingsplicht
Personen in dienst van of werkzaam voor de verwerker hebben een geheimhoudingsplicht.
- Beveiliging
De verwerker treft passende technische en organisatorische maatregelen om de verwerking te beveiligen. Bijvoorbeeld pseudonimisering en versleuteling van persoonsgegevens, permanente informatiebeveiliging, herstel van beschikbaarheid en toegang tot gegevens bij incidenten, regelmatige beveiligingstesten.
- Subverwerkers
De verwerker schakelt geen subverwerker(s) in zonder jouw voorafgaande schriftelijke toestemming. De verwerker legt aan een subverwerker in een subverwerkersovereenkomst dezelfde verplichtingen op als de verwerker richting jou heeft. In de overeenkomst kun je ook direct afspreken dat, en onder welke voorwaarden, de verwerker subverwerkers mag inschakelen. Komt de subverwerker

zijn verplichtingen niet na? Dan blijft de verwerker volledig aansprakelijk richting jou voor het nakomen van de verplichtingen van de subverwerker (zie artikel 28, lid 4 van de AVG).

- Privacyrechten

De verwerker helpt je om te voldoen aan jouw plichten als betrokkenen hun privacyrechten uitoefenen (zoals het recht op inzage, correctie, vergetelheid en dataportabiliteit).

- Andere verplichtingen

De verwerker helpt je ook om andere verplichtingen na te komen. Zoals bij het melden van datalekken, het uitvoeren van een data protection impact assessment (DPIA) en bij een voorafgaande raadpleging.

- Gegevens verwijderen

Na afloop van de verwerkingsdiensten verwijdert de verwerker de gegevens. Of bezorgt hij deze aan jou terug, als jij dat wilt. Ook verwijdert hij kopieën. Tenzij de verwerker wettelijk verplicht is de gegevens te bewaren.

- Audits

De verwerker werkt mee aan jouw audits of die van een derde partij. En stelt alle relevante informatie beschikbaar om te kunnen controleren of hij zich als verwerker houdt aan de hierboven genoemde verplichtingen (uit artikel 28 AVG).

Wij hebben een voorbeeld van een Verwerkersovereenkomst, deze vind je op <https://www.ngsmassage.nl/leden/avg> onder Stap 3 van het Stappenplan. In het voorbeeld kun je de gele vlakken vervangen voor en aanvullen met hetgeen dat op jouw organisatie (medische instelling) van toepassing is.

LET OP: Dit is een voorbeeld document, je kunt hier geen rechten aan ontleen. Je kunt het aanpassen zodat deze meer geschikt is voor jouw situatie. Je blijft zelf verantwoordelijk voor de inhoud en toepassing van dit document.