

Stap 2: Verwerkingsregister en Privacy Policy

Bij 'Stap 1: Inventarisatie Persoonsgegevens' ben je nagegaan welke persoonsgegevens er binnen jouw organisatie (massagepraktijk) gebruikt worden. Bij 'Stap 2: Verwerkingsregister en Privacy Policy' wordt de inventarisatie uitgebreid met de grondslag, verwerking, bewaartermijn en beveiliging van de persoonsgegevens en wordt ondersteuning geboden voor het vastleggen hiervan in een Verwerkingsregister. Ook wordt in deze stap ondersteuning geboden voor het opstellen van een Privacy Policy.

Een organisatie mag persoonsgegevens die voor het ene doel verkregen zijn, niet gebruiken voor een ander doel. Wanneer bijvoorbeeld een e-mailadres is verkregen voor het versturen van de algemene nieuwsbrief, dan mag dit e-mailadres niet gebruikt worden voor andere communicatie. Er is daarvoor immers geen toestemming gevraagd en gekregen, oftewel: daar is geen grondslag voor. Door dus precies alle grondslagen uit te werken, wordt helder wat er precies met welke persoonsgegevens wel en niet mag gebeuren.

De grondslagen en de verwerkingen van persoonsgegevens dienen te worden bijgehouden in een verwerkingsregister, die ter beschikking kan worden gesteld aan de Autoriteit Persoonsgegevens wanneer daarnaar wordt gevraagd. Ook moeten de personen van wie de persoonsgegevens worden verwerkt, dan wel gaan worden verwerkt, goed geïnformeerd worden over hun rechten. Dit gebeurt door middel van een Privacy Policy.

LET OP: - Het is verstandig om zo min mogelijk persoonsgegevens te hanteren. Vraag dus alleen de gegevens die je echt nodig hebt voor het goed functioneren van jouw organisatie (massagepraktijk).

- Een persoon heeft altijd het recht om zijn persoonsgegevens in te zien.

- Overal waar wordt gevraagd om toestemming voor het verwerken van persoonsgegevens of acceptatie van de Privacy Policy geldt: 'Nee is de standaard'. Het antwoord moet dus actief op 'Ja' gezet worden.

Verwerkingsregister

Het verwerkingsregister is een opsomming van de belangrijkste informatie over jouw verwerkingen van persoonsgegevens. Je moet de verwerkingen van persoonsgegevens in het register bijhouden die op dat moment plaatsvinden. Of je ook verplicht verwerkingen moet bijhouden die in het verleden hebben plaatsgevonden wordt niet geheel duidelijk uit de Verordening. Wel is het verstandig met het oog op jouw bewijspositie, om wijzigingen in verwerkingen en gestaakte verwerkingen te archiveren.

Het verwerkingsregister dient in schriftelijke vorm opgesteld te worden. Dit mag ook een register in elektronische vorm zijn en mag dus worden opgemaakt in een tekstverwerkingsbestand, een spreadsheet, speciaal daartoe bestemde software of elke

andere schriftelijke vorm. Wanneer de Autoriteit Persoonsgegevens daarom vraagt moet je haar het register ter beschikking stellen.

In het register neem je niét de daadwerkelijke persoonsgegevens van betrokkenen op! Het register geeft slechts door middel van een beschrijving inzicht in de verwerkingsactiviteiten. Het register bevat dus een beschrijving van de verwerkingsactiviteiten en niét de persoonsgegevens zelf.

Als je jouw verwerkingsactiviteit wijzigt, moet je het register daarop aanpassen. Wanneer je bijvoorbeeld persoonsgegevens die je al verwerkt en in het register hebt beschreven, voor een nieuw doel gaat gebruiken, dan moet je deze nieuwe verwerkingsactiviteit registreren. Maar ook wanneer je de verwerkingsactiviteiten voor dezelfde doeleinden voortzet, alleen met méér of andere gegevens, dan moet je deze nieuwe categorieën persoonsgegevens in het register toevoegen. Het register dient kort gezegd altijd een volledig en actueel overzicht van de hierboven genoemde informatie te bevatten.

Voor het opstellen van het verwerkingsregister hebben wij een voorbeeld gemaakt, deze vind je op www.ngsmassage.nl/leden/avg onder Stap 2 van het Stappenplan. In het voorbeeld kun je de gele vlakken vervangen voor en aanvullen met hetgeen dat op jouw organisatie (massagepraktijk) 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.

Privacy Policy

Middels een Privacy Policy, ook wel bekend als Privacystatement, informeer je mensen op de privacyrechten die zij hebben. De Privacy Policy moet tenminste de volgende informatie bevatten:

- de doelen waarvoor je de gegevens verwerkt;
- de categorieën persoonsgegevens die je van de betrokkene verwerkt;
- de ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of worden doorgegeven, met name ontvangers in derde landen of internationale organisaties;
- indien mogelijk hoe lang je de gegevens bewaart, of indien dat niet mogelijk is, de criteria om de bewaartermijn te bepalen;
- het op recht op wijziging, verwijdering, beperking of bezwaar;
- het recht om een klacht in te dienen bij de toezichthouder;
- wanneer de persoonsgegevens niet bij de betrokkene worden verzameld, alle beschikbare informatie over de bron van die gegevens; en

- het bestaan van geautomatiseerde besluitvorming waaronder profilering, en indien dit het geval is, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

De Privacy Policy van de organisatie (massagepraktijk) moet voor iedereen vindbaar zijn. Het eenvoudigste is om deze op de website van de organisatie (massagepraktijk) te zetten en op elke pagina (onderaan) een link hier naar toe te leggen. Ook moet in alle overeenkomsten (documenten waarin persoonsgegevens gevraagd worden) een verwijzing staan naar de privacy policy.

Wij hebben een voorbeeld van een Privacy Policy, deze vind je op www.ngsmassage.nl/leden/avg onder Stap 2 van het Stappenplan. In het voorbeeld kun je de gele vlakken vervangen voor en aanvullen met hetgeen dat op uw organisatie (massagepraktijk) 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.