Stap 3: Verwerkersovereenkomst

Bij ‘Stap 1: Inventarisatie Persoonsgegevens’ bent u nagegaan welke persoonsgegevens er binnen uw organisatie (medische instelling) gebruikt worden. Bij ‘Stap 2: Verwerkingsregister en Privacy Policy’ heeft u de inventarisatie uitgebreid met de grondslag, verwerking, bewaartermijn en beveiliging van de persoonsgegevens en heeft u dit vastgelegd in een Verwerkingsregister. Ook heeft u een Privacy Policy opgesteld. In deze derde stap, ontvangt u ondersteuning voor het opstellen van verwerkersovereenkomsten.

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

<u>Wanneer is uw organisatie (medische instelling) de ‘verwerkingsverantwoordelijke’?</u>
Wanneer de organisatie (medische instelling) zelf het doel en de middelen voor de verwerking van persoonsgegevens vaststelt, is de organisatie (medische instelling) verwerkingsverantwoordelijke.

<u>Wanneer is uw organisatie (medische instelling) een ‘verwerker’?</u>
Verwerkt de organisatie (medische instelling) in opdracht van een verantwoordelijke persoonsgegevens? Dan is de organisatie (medische instelling) de verwerker.

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

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

Verwerkersovereenkomst

In een verwerkersovereenkomst spreekt u af wat de andere partij met de door u 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 u uit dat de andere partij de persoonsgegevens voor eigen doelen mag verwerken.

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

Let op: als u de gegevensverwerking door een verwerker laat uitvoeren, dan bent u 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 uw rechten en verplichtingen als verwerkingsverantwoordelijke (nu nog ‘verantwoordelijke’ genoemd).
- Instructies verwerking
  De verwerking vindt in principe uitsluitend plaats op basis van uw 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 uw voorafgaande schriftelijke toestemming. De verwerker legt aan een subverwerker in een subverwerkersovereenkomst dezelfde verplichtingen op als de verwerker richting u heeft. In de overeenkomst kunt u 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 u voor het nakomen van de verplichtingen van de subverwerker (zie artikel 28, lid 4 van de AVG).

- Privacyrechten
  De verwerker helpt u om te voldoen aan uw plichten als betrokkenen hun privacyrechten uitoefenen (zoals het recht op inzage, correctie, vergetelheid en dataportabiliteit).
- Andere verplichtingen
  De verwerker helpt u 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 u terug, als u dat wilt. Ook verwijdert hij kopieën. Tenzij de verwerker wettelijk verplicht is de gegevens te bewaren.
- Audits
  De verwerker werkt mee aan uw 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 vindt u op www.sportgeneeskunde.com/algemene-verordening-gegevensbescherming-avg onder Stap 3 van het Stappenplan. In het voorbeeld kunt u de gele vlakken vervangen voor en aanvullen met hetgeen dat op uw organisatie (medische instelling) van toepassing is.

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