Nederlandse Federatie Gezondheidszorg

# Verwerkersovereenkomst

Versie: 20180502

# Verwerkersovereenkomst [Haptotherapie Baak]

Datum: **[9-5-2018]**

Contractspartijen: 1. Verantwoordelijke te weten **[haptotherapie Baak],** statutair gevestigd te **[Nijmegen]**, vertegenwoordigd door **[Laetitia Baak]**

hierna te noemen: “Verantwoordelijke”,

en

2. Verwerker te weten **[uw NAAM],** statutair gevestigd te **[……],** vertegenwoordigd door **[NAAM EN/OF NAAM BESTUURDER]**

hierna te noemen: “Verwerker”,

gezamenlijk aan te duiden als: “Partijen”;

Overwegende dat:

Partijen hebben op **[DATUM]** een Overeenkomst met betrekking tot **[therapie]** gesloten. Ter uitvoering van onze Overeenkomst worden Persoonsgegevens verwerkt.

*Verantwoordelijke hecht grote waarde aan het beschermen van deze Persoonsgegevens, daarom is Verantwoordelijke verantwoordelijk voor de gegevens die Verwerker gaat verwerken en leggen Partijen in deze Verwerkersovereenkomst en de daarbij behorende bijlagen:*

1. *Overzicht met verwerkingen van persoonsgegevens en verwerkingsdoelen*
2. *Overzicht met beveiligingsmaatregelen*
3. *Proces rondom het melden van Datalekken en de te verstrekken informatie*

*vast wat Verwerker wel en niet mag doen met de Persoonsgegevens.*

## Artikel 1. Definities

De hierna en hiervoor gebruikte begrippen volgen uit de Algemene Verordening Gegevensbescherming en hebben de volgende betekenis:

1. Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene”); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon
2. Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;

3. Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen;
4. Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt;
5. Betrokkene: geïdentificeerde of identificeerbaar natuurlijk persoon op wie de verwerkte persoonsgegeven betrekking hebben;
6. Verwerkersovereenkomst: deze overeenkomst inclusief de bijlagen;
7. Overeenkomst: de hoofdovereenkomst waar deze Verwerkersovereenkomst uit voortvloeit;
8. Inbreuk in verband met persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens (“Datalek”);
9. Toezichthoudende autoriteit: een onafhankelijke overheidsinstantie verantwoordelijk voor het toezicht op de naleving van de wet in verband met de verwerking van Persoonsgegevens. In Nederland is dit de Autoriteit Persoonsgegevens;

## Artikel 2. Totstandkoming, duur en beëindiging van deze Verwerkersovereenkomst

1. Deze Verwerkersovereenkomst treedt in werking op de datum waarop Partijen deze ondertekenen.
2. Deze Verwerkersovereenkomst is onderdeel van de Overeenkomst en zal gelden voor zolang de Overeenkomst duurt.
3. Indien de Overeenkomst eindigt, eindigt deze Verwerkersovereenkomst automatisch; de Verwerkersovereenkomst kan niet apart worden opgezegd.
4. Na beëindiging van deze Verwerkersovereenkomst zullen de lopende verplichtingen voor verwerker, zoals het melden van Datalekken, waarbij de Persoonsgegevens van Verantwoordelijke betrokken zijn, en de plicht tot geheimhouding blijven voortduren.

## 3. Verwerken Persoonsgegevens

1. Verwerker zal alleen Persoonsgegevens verwerken in opdracht van Verantwoordelijke en heeft geen zeggenschap over de Persoonsgegevens. Verwerker volgt de instructies van Verantwoordelijke hierover op en mag de Persoonsgegevens niet op een andere manier verwerken, tenzij Verantwoordelijke verwerker daar van te voren toestemming of opdracht voor heeft gegeven.
2. In Bijlage 1 wordt opgenomen welke Persoonsgegevens Verwerker precies zal verwerken en voor welke verwerkingsdoeleinden.
3. Verwerker houdt zich aan de wet en verwerkt de gegevens op een behoorlijke, zorgvuldige en transparante wijze.
4. Verwerker mag zonder voorafgaande schriftelijke toestemming van verantwoordelijke geen andere personen of organisaties inschakelen bij het verwerken van de Persoonsgegevens.

5. Wanneer Verwerker met toestemming van verantwoordelijke andere organisaties inschakelt, moeten zij minimaal voldoen aan de eisen die zijn opgenomen in deze Verwerkersovereenkomst.
6. Wanneer Verantwoordelijke een verzoek krijgt van een Betrokkene die zijn of haar privacy rechten wil uitoefenen, werkt verwerker daar binnen een termijn van 14 dagen aan mee. Deze rechten bestaan uit een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming, bezwaar maken tegen de verwerking van de persoonsgegevens en een verzoek tot overdraagbaarheid van de eigen Persoonsgegevens.

## 4. Beveiligen van Persoonsgegevens

1. Verwerker zorgt ervoor dat de Persoonsgegevens voldoende beveiligd zijn. Om verlies en onrechtmatige verwerkingen te voorkomen neemt Verwerker passende technische en organisatorische maatregelen zoals bedoeld in Artikel 32 AVG.
2. Deze maatregelen zijn afgestemd op het risico van de verwerking. Een overzicht van deze maatregelen en het beleid daarover neemt verwerker op in Bijlage 2.
3. Ter controle zal Verwerker aan Verantwoordelijke ieder jaar een rapportage sturen waarin de genomen maatregelen staan en de eventuele aandachts- en/of verbeterpunten. Hiervoor zal Verwerker aan verantwoordelijke geen kosten in rekening brengen.
4. Verantwoordelijke mag een inspectie of audit in de organisatie van verwerker laten uitvoeren om te bepalen of het verwerken van de Persoonsgegevens aan de wet en de afspraken uit deze Verwerkersovereenkomst voldoet. Hierbij zal Verwerker zijn medewerking verlenen, waaronder het toegang verlenen tot gebouwen en databases en het ter beschikking stellen van alle relevante informatie.
5. De kosten voor de uitvoering van deze audit zullen voor rekening van Verwerker komen wanneer blijkt dat Verwerker zich niet aan de verplichtingen in deze Verwerkersovereenkomst houdt.
6. De controle op de algehele verwerking van Persoonsgegevens door verwerker kan, naast de audit mogelijkheid, ook gebeuren via zelfevaluatie. Verwerker zal hierbij aan Verantwoordelijke een rapport verstrekken waarin Verwerker aantoont dat de activiteiten van Verwerker voldoen aan de wet en de afspraken uit deze Verwerkersovereenkomst. Deze rapportage dient te worden ondertekend door een directielid binnen organisatie van Verwerker.
7. Wanneer één der partijen vindt dat een wijziging in de te nemen beveiligingsmaatregelen noodzakelijk is, treden Partijen in overleg over de wijziging daarvan. De kosten voor het wijzigen van de beveiligingsmaatregelen komen voor de rekening van degene die de kosten maakt.

## 5. Exporteren Persoonsgegevens

1. Verwerker mag geen Persoonsgegevens laten verwerken door andere personen of organisaties buiten de Europese Economische Ruimte (EER), zonder daarvoor voorafgaande toestemming te hebben verkregen van Verantwoordelijke.

## 6. Geheimhouding

1. Verwerker zal de aan de hem/haar verstrekte Persoonsgegevens geheim houden, tenzij dit op basis van een wettelijke verplichting niet mogelijk is.

2. Verwerker zal ervoor zorgdragen dat ook het personeel en ingeschakelde hulppersonen van verwerker zich aan deze geheimhouding houden, door een geheimhoudingsplicht in de (arbeids-) contracten op te nemen.

## 7. Datalekken

1. In geval van een ontdekking van een mogelijk Datalek zal Verwerker Verantwoordelijke hierover informeren binnen 24 uur via **[emailadres en telefoonnummer**] en Verantwoordelijke de informatie verstrekken die is aangegeven in Bijlage 3, zodat Verantwoordelijke indien nodig een melding bij de Toezichthouder kan doen.
2. Na de melding van een Datalek aan Verantwoordelijke dient Verwerker Verantwoordelijke op de hoogte te houden van nieuwe ontwikkelingen rondom het Datalek en de maatregelen die Verwerker heeft getroffen om de omvang van het Datalek te beperken en te beëindigen en een soortgelijk incident in de toekomst te kunnen voorkomen.
3. Het niet toegestaan dat Verwerker een melding van een Datalek doet aan de Toezichthouder en ook mag Verwerker de Betrokkenen niet informeren over het Datalek. Dit is de verantwoordelijkheid van Verantwoordelijke.
4. Eventuele kosten die gemaakt worden om het Datalek op te lossen en in de toekomst te kunnen voorkomen, komen voor rekening van degene die de kosten maakt.

## 8. Aansprakelijkheid

1. Als Verwerker de verplichtingen uit deze Verwerkersovereenkomst niet nakomt, dan zal Verwerker daarvoor aansprakelijk worden gesteld door Verantwoordelijke.
2. Verwerker is aansprakelijk voor alle schade en nadeel geleden door het niet nakomen van de wet en de bepalingen uit deze Verwerkersovereenkomst, voor zover dit is ontstaan door werkzaamheden van Verwerker.
3. Indien Verwerker de verplichtingen in deze Verwerkersovereenkomst overtreedt, is Verwerker aan Verantwoordelijke een direct opeisbare boete verschuldigd van **[BEDRAG]** voor iedere overtreding en **[BEDRAG]** voor iedere dag dat Verwerker de overtreding begaat. Daarnaast behoudt Verantwoordelijke het recht om schadevergoeding te vorderen.
4. Verwerker is aansprakelijk voor de aan Verantwoordelijke opgelegde bestuurlijke boete door de Toezichthouder als de geleden schade het gevolg is van onrechtmatig of nalatig handelen van Verwerker.
5. Verantwoordelijke is niet aansprakelijk voor aanspraken van Betrokkenen of andere personen en organisaties waar Verwerker de samenwerking mee is aangegaan of waarvan Verwerker Persoonsgegevens verwerkt als dit het gevolg is van onrechtmatig of nalatig handelen van Verwerker.

## 9. Teruggave Persoonsgegevens en bewaartermijn

1. Na het beëindigen van deze Verwerkersovereenkomst geeft Verwerker de Persoonsgegevens terug aan Verantwoordelijke. Eventuele achtergebleven Persoonsgegevens dient Verwerker op een zorgvuldige en veilige manier te vernietigen.
2. De Persoonsgegevens die Verwerker verwerkt volgens deze Verwerkersovereenkomst zal vernietigd worden na verstrijken van de wettelijke bewaartermijn en/of op verzoek van Verantwoordelijke.

## 10. Slotbepalingen

1. Deze Verwerkersovereenkomst is onderdeel van de Overeenkomst. Alle rechten en verplichtingen uit de Overeenkomst zijn daarom ook van toepassing op de Verwerkersovereenkomst.
2. Bij eventuele tegenstrijdigheden tussen de bepalingen in de Verwerkersovereenkomst en de Overeenkomst, gelden de bepalingen uit deze Verwerkersovereenkomst.
3. Afwijkingen van deze Verwerkersovereenkomst zijn slechts geldig wanneer Partijen dit samen schriftelijk afspreken.

Aldus door ons overeengekomen en ondertekend:

Verantwoordelijke:

Ondertekend voor en namens

[**haptotherapie Baak]**

Naam:

Functie:

Datum en plaats:

Handtekening:

Bewerker:

Ondertekend voor en namens

**[STATUTAIRE NAAM]**

Naam:

Functie:

Datum en plaats:

Handtekening:

Bijlage 1: Overzicht met verwerkingen van persoonsgegevens en verwerkingsdoelen

| | |
|---|---|
| Beschrijving verwerkingsactiviteiten door Verwerker: | Verwerken van naw gegevens, telefoonnr en emailadres. Informatie w.b. gezondheid en hulpvraag. |
| Verwerkingsdoelen: | Voor een op de persoon afstemde behandeling en versturen van de factuur/vergoeding vanuit verzekering. |
| Verwerkingsverantwoordelijke: | Titia Baak |
| Verwerker: | Titia Baak |
| Sub verwerkers: | Mijn diad administratie systeem. |
| Verwerkte Persoonsgegevens: | Zie boven |
| Locatie verwerkingen: | Mijn diad. |

| | |
|---|---|
| Bewaartermijn: | 15 jaar |

Het onderstaande schema zal ingevuld moeten worden elke keer dat een Verwerkersovereenkomst wordt gesloten. Het geeft een volledig overzicht van de persoonsgegevens die verwerkt zullen worden. Dit maakt het makkelijker om aan te kunnen tonen waar, door wie en voor welk doel de persoonsgegevens worden verwerkt.

## Bijlage 2: Overzicht met beveiligingsmaatregelen

Hier moet een overzicht van de beveiligingsnormen opgenomen worden die de Verwerkingsverantwoordelijke aan de Verwerker oplegt. Om vast te stellen wat passende beveiligingsmaatregelen zijn moet een afweging worden gemaakt op basis van de risico's van de verwerking aan de hand van onder meer de volgende punten:

- Het soort persoonsgegevens dat verwerkt wordt (normaal, bijzonder of gevoelig) en eventueel de daarbij behorende (risico)classificatie die de organisatie zelf aan de gegevens heeft gegeven. Gaat het bijvoorbeeld om een naam of een emailadres, wat minder gevoelige persoonsgegevens zijn, of gaat het om het verwerken van een BSN.
- De hoeveelheid betrokkenen van wie gegevens worden verwerkt. Hoe meer betrokkenen er zijn hoe meer eisen er worden gesteld aan de beveiliging van de gegevens.
- Het doel waarvoor gegevens worden verwerkt.
- De duur en de wijze waarop gegevens bewaard moeten worden. Er kan vervolgens onderscheid gemaakt worden tussen organisatorische beveiligingseisen, zoals het voorkomen van diefstal van een laptop met daarop persoonsgegevens uit de auto, en technische beveiligingseisen, zoals een uitgebreide IT omgeving die beveiligd wordt tegen virussen en waar encryptie van de gegevens wordt toegepast. Van een grote organisatie wordt meer verwacht ten aanzien van de te nemen beveiligingseisen.

**Technische beveiligingsmaatregelen**

☐Up to date virusscan

☐Beveiligde USB-sticks

☐Accurate beveiliging medewerkerstelefoon

☐Bitlocker toegangsmechanisme

☐Unieke inlogcode en wachtwoord (regelmatig aanpassen)

☐Versleutelde email

☐Geen onbeveiligde externe harde schijven

☐Geen onbeveiligde back ups maken

☐Geen documenten op privé laptop opslaan

**Organisatorische beveiligingsmaatregelen**

☐Clean desk policy

☐Laptop niet onbemand achterlaten

☐Laptop nooit achterlaten in de auto

☐Privacy screening medewerkers

☐Oude documenten op juiste manier vernietigen

☐Zorgvuldig gebruik van USB-sticks

**Bijlage 3: Proces rondom het melden van Datalekken en de te verstrekken informatie**

Wat is een beveiligingsincident en wanneer moet dit gemeld worden?

Een datalek is een beveiligingsincident waarbij Persoonsgegevens, die de Verwerker namens de Verwerkingsverantwoordelijke beheert, mogelijk verloren zijn gegaan of onbedoeld toegankelijk waren voor derden. Het gaat om gegevens die te koppelen zijn aan deze personen, zoals, maar niet beperkt tot, namen, adressen, telefoonnummers, e-mailadressen, log in gegevens, cookies, IP adressen of identificerende gegevens van computers of telefoons.

Hieronder vind je een aantal voorbeelden van beveiligingsincidenten die moeten worden gemeld bij de Autoriteit Persoonsgegevens.

- De website met logingegevens is gehackt of is toegankelijk voor derden. - Verlies van een laptop of USB-stick met persoonsgegevens. - Salarisstroken van medewerkers zijn per ongeluk naar verkeerde personen gestuurd. - Brieven of e-mails worden naar een verkeerd adres gestuurd. - Een aanval van een hacker op het ICT systeem. - Een verloren of gestolen telefoon waar persoonsgegevens op aanwezig zijn.

**Wat te doen bij twijfel?**

Als je op basis van bovenstaande niet zeker weet of er sprake is van een beveiligingsincident, stel je jezelf in ieder geval alvast de volgende vragen als hulpmiddel:

- Is er een technisch of fysiek beveiligingsprobleem? - Gaat het probleem over de beveiliging van Persoonsgegevens? Ook IP-adressen, telefoonnummers of identificerende gegevens, bijvoorbeeld van hardware, kunnen hieronder vallen. - Gaat het om gevoelige gegevens zoals ras, gezondheidsgegevens, informatie over iemands financiële situatie, zoals salaris of gegevens waar (identiteits)fraude mee kan worden gepleegd, zoals een Burgerservicenummer. - Zijn er grote hoeveelheden persoonsgegevens onbedoeld toegankelijk geworden voor derden? - Gaat het om gegevens van kwetsbare groepen zoals kinderen? - Worden de persoonsgegevens beheerd door een leverancier?

Ook wanneer je twijfelt, neem het zekere voor het onzekere en neem altijd contact op met **[invoeren naam contactpersoon of afdeling]**.

Waar meld je het beveiligingsincident?

Als je een beveiligingsincident hebt ontdekt, neem je direct contact op met de [invoeren naam contactpersoon of afdeling]:

TEL: [invoeren telefoonnummer]

Of

E-MAIL: [invoeren e-mailadres].