Verwerkersovereenkomst Fysio Topfit



Versie september 2026

Partijen

1. Fysio Topfit, gevestigd aan Vosholplein 1, 2461 AA in Ter Aar, ingeschreven bij de Kamer van Koophandel onder nummer 72707593, rechtsgeldig vertegenwoordigd door Ralph van der Winden, eigenaar,

hierna te noemen: "Verwerkingsverantwoordelijke";

en

2. [Naam verwerker], gevestigd aan [adres], ingeschreven bij de Kamer van Koophandel onder nummer [KvK-nummer], rechtsgeldig vertegenwoordigd door [naam], [functie],

hierna te noemen: "Verwerker";

hierna gezamenlijk te noemen: "Partijen".

Overwegingen

A. Verwerkingsverantwoordelijke is een praktijk voor fysiotherapie en verwerkt in dat kader persoonsgegevens van onder meer patiënten, waaronder gegevens over gezondheid.

B. Partijen hebben een overeenkomst gesloten of maken afspraken over [korte omschrijving van de dienst, bijvoorbeeld: hosting en onderhoud van de website / IT-beheer / administratieve ondersteuning] (hierna: de "Hoofdovereenkomst").

C. Bij de uitvoering van de Hoofdovereenkomst verwerkt Verwerker persoonsgegevens in opdracht van Verwerkingsverantwoordelijke. Verwerker is daarmee verwerker in de zin van artikel 4, onderdeel 8, van de Algemene Verordening Gegevensbescherming (AVG).

D. Partijen willen in deze verwerkersovereenkomst de afspraken vastleggen die artikel 28 AVG voorschrijft.

Partijen komen het volgende overeen:

Artikel 1. Begrippen

1.1 Begrippen in deze overeenkomst, zoals persoonsgegevens, verwerking, betrokkene, verwerkingsverantwoordelijke, verwerker, subverwerker en inbreuk in verband met persoonsgegevens (datalek), hebben de betekenis die de AVG daaraan geeft.

1.2 **Bijzondere persoonsgegevens:** persoonsgegevens als bedoeld in artikel 9 AVG, waaronder gegevens over gezondheid.

Artikel 2. Onderwerp en omvang van de verwerking

2.1 Verwerker verwerkt persoonsgegevens uitsluitend in opdracht van Verwerkingsverantwoordelijke en alleen voor zover dat nodig is voor de uitvoering van de Hoofdovereenkomst.

2.2 Het onderwerp, de duur, de aard en het doel van de verwerking, de soorten persoonsgegevens en de categorieën betrokkenen staan beschreven in Bijlage 1.

2.3 Verwerker verwerkt de persoonsgegevens niet voor eigen doeleinden, zoals marketing, productontwikkeling of het trainen van (AI-)systemen, en verstrekt ze niet aan derden, tenzij Verwerkingsverantwoordelijke daarvoor schriftelijk opdracht heeft gegeven of een wettelijke verplichting dat vereist.

2.4 Verwerker heeft geen zeggenschap over het doel en de middelen van de verwerking. De persoonsgegevens blijven eigendom van Verwerkingsverantwoordelijke.

Artikel 3. Instructies van Verwerkingsverantwoordelijke

3.1 Verwerker verwerkt de persoonsgegevens uitsluitend op basis van schriftelijke instructies van Verwerkingsverantwoordelijke. Deze overeenkomst en de Hoofdovereenkomst gelden als zulke instructies.

3.2 Is Verwerker wettelijk verplicht persoonsgegevens anders te verwerken, dan informeert hij Verwerkingsverantwoordelijke daarover vooraf, tenzij de wet dat verbiedt.

3.3 Is Verwerker van mening dat een instructie in strijd is met de AVG of andere wet- en regelgeving, dan meldt hij dat direct aan Verwerkingsverantwoordelijke.

Artikel 4. Geheimhouding

4.1 Verwerker houdt de persoonsgegevens geheim. Verwerker zorgt ervoor dat alle personen die onder zijn gezag toegang hebben tot de persoonsgegevens, zoals medewerkers en ingehuurde krachten, schriftelijk tot geheimhouding zijn verplicht.

4.2 Verwerker geeft alleen die personen toegang die de gegevens nodig hebben voor hun werkzaamheden (need-to-know).

4.3 De geheimhoudingsplicht blijft ook na het einde van deze overeenkomst gelden.

Artikel 5. Beveiliging

5.1 Verwerker neemt passende technische en organisatorische maatregelen om de persoonsgegevens te beveiligen tegen verlies en onrechtmatige verwerking, zoals bedoeld in artikel 32 AVG. Daarbij houdt Verwerker rekening met het feit dat het om gezondheidsgegevens kan gaan, waarvoor een hoog beveiligingsniveau nodig is.

5.2 De maatregelen die Verwerker in ieder geval neemt, staan in Bijlage 2. Verwerker stemt zijn beveiliging af op de NEN 7510 (informatiebeveiliging in de zorg) of een gelijkwaardige norm, zoals ISO 27001.

5.3 Verwerker evalueert en verbetert de maatregelen regelmatig. Verwerker informeert Verwerkingsverantwoordelijke over wijzigingen die het beveiligingsniveau verlagen, en voert die niet door zonder schriftelijke toestemming.

Artikel 6. Subverwerkers

6.1 Verwerker schakelt geen subverwerker in zonder voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke. De subverwerkers waarvoor bij het sluiten van deze overeenkomst toestemming is gegeven, staan in Bijlage 3.

6.2 Wil Verwerker een subverwerker toevoegen of vervangen, dan meldt hij dat ten minste 30 dagen van tevoren schriftelijk aan Verwerkingsverantwoordelijke. Verwerkingsverantwoordelijke kan binnen die termijn met redenen omkleed bezwaar maken. Bij bezwaar zoeken Partijen samen naar een oplossing. Lukt dat niet, dan mag Verwerkingsverantwoordelijke de Hoofdovereenkomst en deze overeenkomst kosteloos beëindigen.

6.3 Verwerker legt aan elke subverwerker schriftelijk ten minste dezelfde verplichtingen op als die in deze overeenkomst staan.

6.4 Verwerker blijft tegenover Verwerkingsverantwoordelijke volledig aansprakelijk voor het handelen en nalaten van zijn subverwerkers.

Artikel 7. Doorgifte buiten de Europese Economische Ruimte

7.1 Verwerker verwerkt de persoonsgegevens uitsluitend binnen de Europese Economische Ruimte (EER), tenzij Verwerkingsverantwoordelijke vooraf schriftelijk toestemming heeft gegeven voor doorgifte naar een land daarbuiten.

7.2 Toestemming wordt alleen gegeven als de doorgifte voldoet aan hoofdstuk V van de AVG, bijvoorbeeld op basis van een adequaatheidsbesluit van de Europese Commissie (zoals het EU-VS Data Privacy Framework voor gecertificeerde organisaties) of de standaardcontractbepalingen van de Europese Commissie, zo nodig aangevuld met extra maatregelen.

7.3 Verwerker vermeldt in Bijlage 3 per subverwerker waar de gegevens worden verwerkt en, bij doorgifte buiten de EER, op welke grondslag.

Artikel 8. Datalekken

8.1 Verwerker informeert Verwerkingsverantwoordelijke zonder onredelijke vertraging, en uiterlijk binnen 24 uur na ontdekking, telefonisch én per e-mail over elk (vermoedelijk) datalek of beveiligingsincident dat betrekking heeft op de persoonsgegevens. De contactgegevens staan in Bijlage 1.

8.2 Verwerker verstrekt daarbij, voor zover bekend, ten minste de volgende informatie:

- de aard van het incident en wanneer het heeft plaatsgevonden en is ontdekt;
- de soorten persoonsgegevens die betrokken zijn, waaronder of het gaat om gezondheidsgegevens of het BSN;
- het (geschatte) aantal betrokkenen en gegevensbestanden;
- de waarschijnlijke gevolgen van het incident;
- de maatregelen die zijn genomen of worden voorgesteld om het incident te beëindigen en de gevolgen te beperken;
- de contactpersoon bij Verwerker voor verdere informatie.

8.3 Is nog niet alle informatie beschikbaar, dan verstrekt Verwerker die zo snel mogelijk aanvullend. Zo kan Verwerkingsverantwoordelijke binnen 72 uur beoordelen of een melding aan de Autoriteit Persoonsgegevens en/of de betrokkenen nodig is.

8.4 Verwerker neemt direct alle redelijke maatregelen om het incident te beëindigen en de gevolgen te beperken, en volgt de instructies van Verwerkingsverantwoordelijke op. Verwerker houdt een register bij van alle incidenten.

8.5 Het doen van meldingen aan de Autoriteit Persoonsgegevens en aan betrokkenen is voorbehouden aan Verwerkingsverantwoordelijke.

Artikel 9. Rechten van betrokkenen

9.1 Verwerker helpt Verwerkingsverantwoordelijke bij het afhandelen van verzoeken van betrokkenen om hun rechten uit te oefenen, zoals bedoeld in de artikelen 15 tot en met 22 AVG (onder meer inzage, correctie, verwijdering en dataportabiliteit).

9.2 Ontvangt Verwerker zo'n verzoek rechtstreeks van een betrokkene, dan stuurt hij het binnen 3 werkdagen door naar Verwerkingsverantwoordelijke en handelt hij het niet zelf af, tenzij Verwerkingsverantwoordelijke daartoe opdracht geeft.

Artikel 10. Overige bijstand

10.1 Verwerker helpt Verwerkingsverantwoordelijke, rekening houdend met de aard van de verwerking en de beschikbare informatie, bij het nakomen van de verplichtingen uit de artikelen 32 tot en met 36 AVG. Het gaat daarbij om de beveiliging, het melden van datalekken, het uitvoeren van een gegevensbeschermingseffectbeoordeling (DPIA) en een eventuele voorafgaande raadpleging van de Autoriteit Persoonsgegevens.

10.2 Verwerker werkt mee aan verzoeken of onderzoeken van de Autoriteit Persoonsgegevens of een andere toezichthouder.

Artikel 11. Informatie en audits

11.1 Verwerker stelt alle informatie beschikbaar die nodig is om aan te tonen dat hij zich aan deze overeenkomst en artikel 28 AVG houdt, zoals certificaten (bijvoorbeeld NEN 7510 of ISO 27001) of onafhankelijke auditrapporten.

11.2 Verwerkingsverantwoordelijke mag, na een aankondiging van ten minste 14 dagen, een audit of inspectie laten uitvoeren door zichzelf of een onafhankelijke deskundige die tot geheimhouding is verplicht. Verwerker werkt daaraan mee. De kosten van de audit zijn voor Verwerkingsverantwoordelijke, tenzij blijkt dat Verwerker deze overeenkomst op wezenlijke punten niet nakomt.

Artikel 12. Aansprakelijkheid

12.1 Verwerker is aansprakelijk voor schade en boetes die het gevolg zijn van het niet nakomen van deze overeenkomst of van de AVG door Verwerker of zijn subverwerkers, zoals bepaald in artikel 82 AVG.

12.2 Verwerker vrijwaart Verwerkingsverantwoordelijke voor aanspraken van derden, waaronder betrokkenen en toezichthouders, die het gevolg zijn van zo'n tekortkoming.

12.3 Een eventuele beperking van aansprakelijkheid in de Hoofdovereenkomst geldt niet voor schade als gevolg van opzet of grove schuld, of van het overtreden van de artikelen 4 (geheimhouding), 5 (beveiliging), 7 (doorgifte) en 8 (datalekken) van deze overeenkomst.

Artikel 13. Duur en beëindiging

13.1 Deze overeenkomst gaat in op de datum van ondertekening en loopt zolang de Hoofdovereenkomst loopt. Zolang Verwerker na het einde van de Hoofdovereenkomst nog persoonsgegevens voor Verwerkingsverantwoordelijke verwerkt, blijft deze overeenkomst gelden.

13.2 Bij het einde van de dienstverlening geeft Verwerker, naar keuze van Verwerkingsverantwoordelijke, alle persoonsgegevens terug in een gangbaar bestandsformaat en/of verwijdert hij ze, inclusief alle kopieën en back-ups, binnen 30 dagen. Dit geldt niet voor zover Verwerker wettelijk verplicht is gegevens te bewaren.

13.3 Verwerker bevestigt de verwijdering schriftelijk aan Verwerkingsverantwoordelijke en zorgt ervoor dat ook zijn subverwerkers de gegevens verwijderen.

13.4 Bepalingen die naar hun aard bedoeld zijn om na het einde van deze overeenkomst te blijven gelden, zoals geheimhouding en aansprakelijkheid, blijven van kracht.

Artikel 14. Slotbepalingen

14.1 Bij strijdigheid tussen deze overeenkomst en de Hoofdovereenkomst gaat deze overeenkomst voor wat betreft de verwerking van persoonsgegevens. Bij strijdigheid tussen deze overeenkomst en de bijlagen gaat de overeenkomst voor.

14.2 Wijzigingen van deze overeenkomst zijn alleen geldig als Partijen ze schriftelijk zijn overeengekomen. Wijzigt de wet- of regelgeving, dan passen Partijen deze overeenkomst zo nodig in onderling overleg aan.

14.3 Is een bepaling nietig of vernietigbaar, dan blijven de overige bepalingen gelden. Partijen vervangen de ongeldige bepaling dan door een geldige bepaling die zo veel mogelijk aansluit bij de bedoeling.

14.4 Op deze overeenkomst is Nederlands recht van toepassing. Geschillen worden voorgelegd aan de bevoegde rechter van de rechtbank [Den Haag].

Ondertekening

Aldus overeengekomen en in tweevoud ondertekend:

Verwerkingsverantwoordelijke	**Verwerker**
Fysio Topfit	[Naam verwerker]
Naam: _____	Naam: _____
Functie: _____	Functie: _____
Plaats: _____	Plaats: _____
Datum: _____	Datum: _____
Handtekening:	Handtekening:
_____	_____

Bijlage 1 – Beschrijving van de verwerking

Vul per verwerker in. Schrap wat niet van toepassing is.

Onderdeel	Omschrijving
Dienstverlening	[bijvoorbeeld: hosting en onderhoud van de website fysiotopfit.nl / IT-beheer / administratieve ondersteuning]
Doel van de verwerking	[bijvoorbeeld: het technisch beschikbaar houden van de website en de contactformulieren]
Aard van de verwerking	[bijvoorbeeld: opslaan, bewaren, raadplegen, verwijderen]
Categorieën betrokkenen	[ ] patiënten (en hun wettelijk vertegenwoordigers) [ ] websitebezoekers [ ] medewerkers [ ] verwijzers en andere zorgverleners
Soorten persoonsgegevens	[ ] NAW-gegevens, telefoonnummer, e-mailadres [ ] geboortedatum en geslacht [ ] verzekeringsgegevens [ ] burgerservicenummer (BSN) [ ] gegevens over gezondheid (bijzondere persoonsgegevens) [ ] IP-adressen en gebruiksgegevens [ ] overig: _____
Duur van de verwerking	Zolang de Hoofdovereenkomst loopt
Locatie van de verwerking	[land / datacentrum]
Contactpersoon Verwerkingsverantwoordelijke (ook voor datalekken)	[naam], Fysio Topfit Telefoon: [nummer] E-mail: [e-mailadres]
Contactpersoon Verwerker	[naam] Telefoon: [nummer] E-mail: [e-mailadres]

Bijlage 2 – Beveiligingsmaatregelen

Verwerker heeft ten minste de volgende maatregelen genomen. Vink aan wat van toepassing is en vul aan waar nodig. Heeft Verwerker een certificaat (bijvoorbeeld NEN 7510 of ISO 27001)? Voeg dan een kopie toe of vermeld het certificaatnummer.

Certificering

[ ] NEN 7510 [ ] ISO 27001 [ ] anders: _____ Certificaatnummer en geldig tot: _____

Technische maatregelen

- [ ] Versleuteling (encryptie) van gegevens bij opslag en tijdens verzending (bijvoorbeeld TLS/https)
- [ ] Toegang alleen met persoonlijke accounts, sterke wachtwoorden en tweestapsverificatie (MFA)
- [ ] Autorisaties op basis van functie (alleen toegang tot gegevens die nodig zijn)
- [ ] Logging van toegang tot en wijzigingen in persoonsgegevens
- [ ] Firewalls, actuele virusscanners en tijdig installeren van beveiligingsupdates
- [ ] Regelmatige back-ups, versleuteld opgeslagen, met periodieke hersteltest
- [ ] Periodieke kwetsbaarheidsscans of penetratietests
- [ ] Veilige verwijdering van gegevens en gegevensdragers

Organisatorische maatregelen

- [ ] Geheimhoudingsverklaring voor alle medewerkers en ingehuurde krachten
- [ ] Verklaring Omtrent het Gedrag (VOG) of andere screening van medewerkers met toegang
- [ ] Periodieke training in informatiebeveiliging en privacy
- [ ] Vastgelegd informatiebeveiligingsbeleid en een procedure voor datalekken
- [ ] Fysieke beveiliging van kantoren, serverruimtes en apparatuur
- [ ] Clean desk- en clear screenbeleid
- [ ] Direct intrekken van toegangsrechten bij uitdiensttreding

Aanvullende maatregelen

_____

_____

Bijlage 3 – Goedgekeurde subverwerkers

Verwerkingsverantwoordelijke geeft toestemming voor de inzet van de onderstaande subverwerkers. Nieuwe subverwerkers worden gemeld volgens artikel 6.2.

Naam subverwerker	Dienst / rol	Locatie verwerking	Grondslag doorgifte (bij buiten EER)

[ ] Verwerker maakt geen gebruik van subverwerkers.