Verwerkersovereenkomst

Inhoudsopgave

Onderwerp	Pagina
1. Partijen	Pagina 2
2. Belang van afspraken	Pagina 2
Artikel 1 - Inhoud afspraken	Pagina 2
Artikel 2 - Verantwoordelijkheden	Pagina 3
Artikel 3 - Beveiliging gegevens	Pagina 3
Artikel 4 - Geheimhouding	Pagina 3
Artikel 5 - Datalek	Pagina 4
Artikel 6 - Externe partijen (onderaannemers)	Pagina 4
Artikel 7 - Rechten van patiënten en medewerkers	Pagina 4
Artikel 8 - Controle en toetsing	Pagina 4
Artikel 9 - Einde van de samenwerking	Pagina 4
Artikel 10 - Aansprakelijkheid	Pagina 5
Bijlage 1 - De opdracht en de gegevens	Pagina 6
Bijlage 2 - Hoe we de gegevens beveiligen	Pagina 8

1. Partijen

Ondertekenaars van dit document:

1. _____ gevestigd in _____ ingeschreven bij de KvK onder nummer _____ hier vertegenwoordigd door _____ (hierna: de **"opdrachtgever"**);

en

2. Doorsteve.nl, gevestigd in Cuijk, Lavendel 452 5432 DX, ingeschreven bij de KvK onder nummer 97715115, hier vertegenwoordigd door Steve Oakes (hierna: de "**opdrachtnemer**");

Samen de **"partijen"**.

De situatie is als volgt:

- Partijen hebben al afspraken gemaakt over de opdracht (de "hoofdovereenkomst").
- De hoofdovereenkomst is de schriftelijke vastlegging van de opdracht, zijnde de geaccepteerde offerte, de opdrachtbevestiging of een andere ondertekende overeenkomst, waarbij ook telefonisch gegeven opdrachten als geldig worden beschouwd.
- Voor deze opdracht krijgt de opdrachtnemer toegang tot gevoelige gegevens van cliënten en medewerkers.

2. Belang van afspraken

We maken deze afspraken om te voldoen aan de privacywetgeving (AVG). Dit contract regelt hoe de opdrachtnemer met de persoonsgegevens omgaat en wie waarvoor verantwoordelijk is, zodat de privacy van de patiënten en medewerkers goed beschermd blijft.

Artikel 1 - Inhoud afspraken

1. Deze overeenkomst regelt hoe de opdrachtnemer de persoonsgegevens verwerkt ten behoeve van de opdrachtgever, in het kader van de hoofdovereenkomst.
2. De opdrachtnemer heeft voor de uitvoering van de opdracht toegang tot alle benodigde documenten en informatie, inclusief bedrijfs- en kwaliteitsdocumenten van de opdrachtgever.
3. Deze afspraken gelden zolang de opdracht duurt, of voor onbepaalde tijd, en gaan in zodra de opdrachtnemer begint met de eerste dienst voor de opdrachtgever.
4. De specifieke werkzaamheden, de aard van de gegevens en de verwerkingsdoelen staan beschreven in bijlage 1.

Artikel 2 - Verantwoordelijkheden

2.1 Verantwoordelijkheid opdrachtgever

a. De opdrachtgever is eindverantwoordelijk over de eigen systemen en IT-infrastructuur.
b. De opdrachtgever is eindverantwoordelijk voor de naleving van de privacywetgeving (AVG).
c. De opdrachtgever is verantwoordelijk voor de wettelijke basis voor de gegevensverwerking en zorgt dat medewerkers de privacyregels volgen.
d. De opdrachtgever is altijd verantwoordelijk voor de juiste opleiding en training van haar personeel dat werkt met de systemen en/of applicaties.
e. Als de opdrachtgever constateert dat de opleiding of training onvoldoende is, moet dit onmiddellijk aan de opdrachtnemer gemeld worden.
f. De opdrachtnemer zal een voorstel doen voor aanvullende training. De kosten hiervoor zijn volledig voor rekening van de opdrachtgever.

2.2 Verantwoordelijkheid opdrachtnemer

a. De opdrachtnemer is verantwoordelijk voor de veilige uitvoering van de specifieke opdrachten.
b. De opdrachtnemer verwerkt gegevens alleen volgens de instructies van de opdrachtgever en nooit voor eigen gebruik.
c. De opdrachtnemer zet zich maximaal in en voert de werkzaamheden met de grootste zorgvuldigheid uit. De opdrachtnemer kan echter niet garanderen dat de geleverde informatie, ondersteuning of het advies in alle omstandigheden volledig of actueel is.
d. De opdrachtgever is bekend met de integriteitscode van opdrachtnemer. Opdrachtnemer zal opdrachten (tussentijds) weigeren als deze met de code in strijd zijn.

2.3 Vrijwaring opdrachtnemer

a. De opdrachtnemer is niet aansprakelijk voor schade die ontstaat doordat de opdrachtgever verkeerde of onjuiste gegevens aanlevert of onjuiste instructies geeft.
b. De opdrachtgever moet de opdrachtnemer verdedigen en de kosten betalen als derden (cliënten, medewerkers) schade claimen door de onjuistheid van de aangeleverde gegevens of instructies.

Artikel 3 - Beveiliging gegevens

1. De opdrachtnemer neemt passende technische en organisatorische maatregelen (T.O.M.) om de gegevens te beveiligen (zie bijlage 2).
2. De beveiliging voldoet minimaal aan de NEN 7510 eisen voor de zorgsector.
3. De opdrachtnemer zorgt zelf voor de beveiliging van de eigen laptops, netwerken en apparatuur en heeft dit ook vastgelegd in zijn eigen beleidsdocumenten.
4. De opdrachtgever is zelf verantwoordelijk voor het beheer en de juistheid van de toegangsrechten van haar medewerkers.

Artikel 4 - Geheimhouding

Iedereen die namens de opdrachtnemer of opdrachtgever met persoonsgegevens werkt, moet geheimhouding beloven. Dit is net zo streng als het beroepsgeheim in de zorg.

Artikel 5 - Datalek

1. De opdrachtnemer meldt een (vermoedelijk) datalek onmiddellijk aan de opdrachtgever, binnen uiterlijk 24 uur na ontdekking.
2. De opdrachtnemer geeft alle nodige informatie zodat de opdrachtgever het lek kan melden bij de Autoriteit Persoonsgegevens en eventueel de betrokkenen.
3. De opdrachtgever meldt een (vermoedelijk) datalek onmiddellijk aan de opdrachtnemer, binnen uiterlijk 24 uur na ontdekking.
4. De opdrachtgever geeft alle nodige informatie zodat de opdrachtgever het lek kan melden bij de Autoriteit Persoonsgegevens en eventueel de betrokkenen.

Artikel 6 - Externe partijen (onderaannemers)

1. De opdrachtnemer zal de overeengekomen werkzaamheden in eerste instantie zonder inschakeling van subverwerkers verrichten.
2. De opdrachtnemer mag alleen andere partijen inschakelen voor de verwerking van gegevens (subverwerkers) met voorafgaande schriftelijke toestemming van de opdrachtgever.
3. Indien voor de uitvoering van de opdracht het inschakelen van een externe partij of derde noodzakelijk is, dan rust de verplichting tot het contracteren van deze partij bij de opdrachtgever.
4. De opdrachtgever is in dat geval zelf volledig verantwoordelijk voor de afspraken met die externe partij en vrijwaart de opdrachtnemer van enige aansprakelijkheid voor het handelen of nalaten van deze door de opdrachtgever ingeschakelde derden.

Artikel 7 - Rechten van cliënten en medewerkers

1. Als cliënten of medewerkers hun privacyrechten willen uitoefenen (zoals inzage of verwijdering), helpt de opdrachtnemer de opdrachtgever hierbij.
2. Als een betrokkene de opdrachtnemer direct benadert, stuurt de opdrachtnemer het verzoek direct door naar de opdrachtgever.

Artikel 8 - Controle en toetsing

De opdrachtgever mag laten controleren of de opdrachtnemer zijn werk goed heeft gedaan, bijvoorbeeld via een externe audit. De opdrachtnemer werkt hier volledig aan mee. Deze controle dient uitsluitend ter kwaliteitsverbetering van de opdrachtgever en/of opdrachtnemer. De opdrachtgever kan aan de uitkomsten van deze controle geen (nieuwe) rechten ontlenen in het kader van aansprakelijkheid van de opdrachtnemer voor het uitgevoerde werk.

Artikel 9 - Einde van de samenwerking

1. De opdrachtnemer heeft het recht deze overeenkomst met onmiddellijke ingang op te zeggen of te ontbinden, indien de opdrachtgever in strijd handelt met de integriteitscode of geldende wet- en regelgeving, en dit een onaanvaardbaar risico vormt voor de opdrachtnemer.
2. Indien de opdrachtgever opzegt, worden lopende opdrachten niet direct beëindigd. Partijen overleggen eerst over de verantwoorde en efficiënte afronding.

3. Als er geen overeenstemming is, heeft de opdrachtnemer het recht de lopende opdrachten af te maken conform de hoofdovereenkomst, en is de opdrachtgever volledig betalingsplichtig.
4. Als de hoofdovereenkomst stopt, moet de opdrachtnemer alle persoonsgegevens van de opdrachtgever verwijderen of terugsturen, tenzij de wet anders bepaalt. Dit moet binnen 30 dagen gebeuren.

Artikel 10 - Aansprakelijkheid

1. De opdrachtnemer is uitsluitend aansprakelijk voor directe schade die het aantoonbare en rechtstreekse gevolg is van een toerekenbare tekortkoming in de uitvoering van de overeengekomen werkzaamheden.
2. De aansprakelijkheid van de opdrachtnemer is te allen tijde beperkt tot de vergoeding die de opdrachtgever voor de betreffende opdracht heeft voldaan.
3. Aansprakelijkheid van de opdrachtnemer voor indirecte schade, waaronder gevolgschade, gederfde winst, gemiste besparingen, en schade door bedrijfsstagnatie, is uitgesloten.
4. De in dit artikel genoemde beperkingen gelden niet indien de schade het gevolg is van opzet of bewuste roekeloosheid van de opdrachtnemer.
5. Indien over de aansprakelijkheid door opdrachtgever een geschil ontstaat, is de opdrachtgever verplicht een onafhankelijk feitenonderzoek te laten uitvoeren, waarvan de kosten volledig voor zijn rekening komen.

Afsluiting en ondertekening

Partijen verklaren de bepalingen van dit document te hebben gelezen en akkoord te gaan met de inhoud daarvan.

De opdrachtgever:	**De opdrachtnemer:**
Naam	Naam
_____	_____
Handtekening	Handtekening
_____	_____
Datum	Datum
_____	_____

Bijlage 1 - De opdracht en de gegevens

Het doel van de verwerking is het ondersteunen van de kerntaken van de opdrachtgever, met een zware nadruk op de interne kwaliteitsborging, compliance en efficiënte bedrijfsvoering.

1. Doeleinden van de verwerking

De verwerking is noodzakelijk voor de volgende doelen:

a. **Ondersteuning en structurering**

   Ondersteuning van de bedrijfsvoering en de IT-processen, inclusief het implementeren en structureren van informatie(systemen).

b. **Kwaliteitsborging en naleving**

   Controleren van de kwaliteit en inhoud van zorg- en personeelsdossiers, kwaliteits- en beleidsdocumenten.

c. **Advisering en Compliance**

   Advisering van de opdrachtgever over audits en wettelijke vereisten (o.a. AVG, WGBO/Wkkgz)

d. **Kennisborging**

   Het verzorgen van scholing en training om interne processen, kwaliteitseisen en wettelijke procedures over te dragen aan het personeel.

2. Categorieën betrokkenen

De opdrachtnemer verwerkt persoonsgegevens van de volgende categorieën personen namens de opdrachtgever:

- Cliënten van de opdrachtgever.
- Personeel (medewerkers) van de opdrachtgever.

3. Soorten persoonsgegevens

De verwerking omvat (onder andere) de volgende soorten persoonsgegevens, waarbij de nadruk ligt op de verwerking van bijzondere en gevoelige gegevens:

Categorie van gegevens	Beschrijving	Wettelijke gevoeligheid
1. Gezondheidsgegevens	Zorgdossiers, cliëntgegevens, medische dossiers.	Bijzonder (Art. 9 AVG)
2. Identificatiegegevens	Burgerservicenummer (BSN), NAW-gegevens, contactgegevens, geboortedatum.	Hoog (BSN vereist extra maatregelen)
3. Personeelsgegevens	Gegevens uit personeelsdossiers, inclusief arbeidscontracten, opleidingen en functie-informatie.	Regulier persoonsgegeven
4. Financiële gegevens	Gegevens met betrekking tot salaris, vergoedingen of declaraties.	Regulier persoonsgegeven

4. Aard van de Verwerking

De verwerker verricht alle verwerkingsactiviteiten die noodzakelijk zijn om de onder punt 1 genoemde doeleinden te bereiken. Dit betreft de volledige levenscyclus van de gegevens:

1. **Gegevensbeheer**

   Verzamelen, vastleggen, ordenen, opslaan, structureren, muteren, verstrekken, raadplegen en vernietigen van gegevens.

2. **Procescontrole**

   Controleren op volledigheid en naleving van de wet en adviseren over beleidsdocumenten.

3. **Educatie**

   Het ontwikkelen en verzorgen van scholing met betrekking tot de verwerkingsprocessen, kwaliteitsstandaarden en compliance-eisen.

Bijlage 2 - Hoe we de gegevens beveiligen (T.O.M)

T.O.M. staat voor Technische en Organisatorische Maatregelen. Dit is de term die in de Algemene Verordening Gegevensbescherming (AVG/GDPR) wordt gebruikt om aan te geven hoe persoonsgegevens worden beschermd. Het gaat om een verplichte, dubbele aanpak.

2.1 De opdrachtnemer (verwerker) zal:

a. Direct en permanent T.O.M. handhaven ter bescherming van de data tegen inbreuken, gericht op de vertrouwelijkheid, integriteit en beschikbaarheid van de data.
b. De volledige en gedetailleerde T.O.M. schriftelijk vastleggen en deze op verzoek direct aan de opdrachtgever verstrekken.
c. Zorgen dat alleen geautoriseerd en getraind personeel toegang heeft tot de data (need-to-know), en dit personeel aan strikte geheimhouding binden.
d. Onverwijld elke inbreuk op de beveiliging of dataverlies aan de opdrachtgever melden en meewerken aan herstel.
e. Zich houden aan onderstaande beveiligingsmaatregelen.

2.2 De opdrachtgever (verwerkingsverantwoordelijke) zal:

a. De opdrachtnemer voorzien van alle noodzakelijke informatie over de aard, omvang en gevoeligheid van de te verwerken data.
b. Het recht uitoefenen om de nageleefde T.O.M. van de opdrachtnemer periodiek te controleren (via audits conform de hoofdovereenkomst).
c. De opdrachtnemer gemotiveerd verzoeken de T.O.M. te wijzigen indien deze niet meer voldoen aan de wettelijke eisen of de actuele stand van de techniek.
d. Zelf verantwoordelijk blijven voor de veilige omgang met eigen inloggegevens en data die zij aan de opdrachtnemer verstrekt.
e. Zich houden aan onderstaande beveiligingsmaatregelen.

2.3 Beveiligingsmaatregelen

a. Gebruik van Twee-Factor Authenticatie (2FA) en sterke wachtwoorden. Toegang is beperkt tot het 'Need-to-know'-principe (alleen wie het nodig heeft) en autorisaties worden actueel gehouden.
b. Gevoelige data wordt versleuteld (Encryptie), zowel bij opslag als overdracht.
c. Alle software en systemen worden tijdig bijgewerkt om kwetsbaarheden te dichten.
d. Er worden regelmatige back-ups gemaakt en er is een plan om systemen snel te herstellen na storingen.
e. Alle activiteiten worden nauwkeurig gelogd (Audit Trails) om afwijkingen in de data-integriteit te kunnen traceren.