Verwerkersovereenkomst HCI

Overwegende dat:

A. Verwerkingsverantwoordelijke en Verwerker een overeenkomst hebben gesloten waarbij Verwerker mogelijk bepaalde Persoonsgegevens dient te Verwerken namens de Verwerkingsverantwoordelijke (de "**Overeenkomst**"); en
B. deze Verwerkersovereenkomst de voorwaarden en de respectievelijke rechten en verplichtingen van partijen bevat ten aanzien van deze Verwerking van Persoonsgegevens.

1 Definities en interpretatie

1.1 In deze Verwerkersovereenkomst hebben de met een hoofdletter geschreven begrippen de betekenis die daar hieronder aan wordt gegeven:

- **AVG** betekent de Algemene Verordening Gegevensbescherming (Verordening (EU) 2016/679).
- **Betrokkene** betekent een geïdentificeerde of identificeerbare natuurlijke persoon.
- **Gegevensbeschermingswetgeving** betekent de AVG en alle wet- en regelgeving die regels bevat voor de bescherming van personen met betrekking tot de Verwerking van Persoonsgegevens.
- **Persoonsgegevens** betekent alle informatie over een Betrokkene die Verwerker namens Verwerkingsverantwoordelijke Verwerkt in het kader van de uitvoering van de Overeenkomst.
- **Subverwerker** betekent een door Verwerker ingeschakelde onderaannemer die toegang heeft of kan hebben tot Persoonsgegevens.
- **Toezichthoudende Autoriteit** betekent een overheidsinstantie of toezichthoudende autoriteit aan wiens toezicht partijen of de Verwerking op enig moment onderhevig kunnen zijn.
- **Verwerkingsverantwoordelijke** betekent U, de partij die, alleen of samen met anderen, het doel en de middelen voor de Verwerking vaststelt.
- **Verwerker** betekent de desbetreffende HCI entiteit, die Persoonsgegevens Verwerkt namens de Verwerkingsverantwoordelijke.
- **Verwerking** of **Verwerken** betekent elke bewerking of een geheel van bewerkingen met betrekking tot 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.
- **Verwerkersovereenkomst** betekent deze gegevensverwerkersovereenkomst tussen Verwerker en Verwerkingsverantwoordelijke met inbegrip van alle bijlagen.

1.2 In geval van strijdigheid tussen deze Verwerkersovereenkomst en de Overeenkomst, prevaleert deze Verwerkersovereenkomst.

2 VERWERKING

2.1 Verwerkingsverantwoordelijke blijft de Verwerkingsverantwoordelijke voor alle Persoonsgegevens die in het kader van de Overeenkomst worden Verwerkt. Verwerker zal uitsluitend ten behoeve van het verlenen van de diensten zoals vastgelegd in de Overeenkomst de categorieën Persoonsgegevens verwerken zoals vermeld in **Bijlage 1** van deze Verwerkersovereenkomst.

3 VERPLICHTINGEN VAN DE VERWERKINGSVERANTWOORDELIJKE

3.1 Verwerkingsverantwoordelijke geeft Verwerker de opdracht om de Persoonsgegevens namens Verwerkingsverantwoordelijke en in overeenstemming met de Gegevensbeschermingswetgeving te Verwerken. De Verwerkingsinstructies van de Verwerkingsverantwoordelijke zijn vastgelegd in Bijlage 1 van de Verwerkersovereenkomst en worden nader omschreven in deze Verwerkersovereenkomst.

3.2 Verwerkingsverantwoordelijke kan aanvullende instructies verstrekken met betrekking tot de Verwerking door Verwerker of de instructies in Bijlage 1 of de Verwerkersovereenkomst wijzigen, mits dergelijke instructies (i) in overeenstemming zijn met de voorwaarden van de Overeenkomst en deze Verwerkersovereenkomst, (ii) redelijk zijn en (iii) in overeenstemming zijn met de Gegevensbeschermingswetgeving. Partijen leggen de door Verwerkingsverantwoordelijke gegeven (aanvullende) instructies schriftelijk vast.

4 VERPLICHTINGEN VAN DE VERWERKER

4.1 Verwerker zal bij de uitvoering van de verplichtingen uit de Overeenkomst:

(i) voldoen aan haar verplichtingen op grond van de Gegevensbeschermingswetgeving en zoals uiteengezet in deze Verwerkersovereenkomst;

(ii) voor rekening van Verwerkingsverantwoordelijke alle redelijkerwijs vereiste informatie en medewerking verlenen:

(a) ten behoeve van het uitvoeren van een gegevensbeschermingseffectenbeoordeling (DPIA); en

(b) mogelijke voorafgaande raadpleging bij een Toezichthoudende Autoriteit,

(iii) de Verwerkingsverantwoordelijke in kennis stellen van elk van de volgende gevallen:

(a) Verwerker een klacht, geschil of verzoek van een Betrokkene ontvangt, behalve in het geval dat Verwerker anderszins wettelijk verplicht is dergelijke informatie niet te verstrekken; en/of

(b) Verwerker een juridisch bindend verzoek van een overheidsinstelling, met inbegrip van gerechtelijke autoriteiten, ontvangt met betrekking tot de Verwerking van Persoonsgegevens onder deze Verwerkersovereenkomst, indien wettelijk toegestaan.

4.2 Verwerker houdt de Persoonsgegevens vertrouwelijk. Verwerker zal de Persoonsgegevens niet verstrekken aan een derde zonder voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke, tenzij, (i) verstrekking verplicht is of nodig ten behoeve van de Verwerking, of (ii) wanneer Persoonsgegevens verstrekt moeten worden aan de bevoegde Toezichthoudende Autoriteit om te voldoen aan een wettelijke verplicht of vereist is voor fiscale doeleinden. Verwerker verzekert zich ervan dat elke bevoegde werknemer die toegang heeft tot de Persoonsgegevens die namens Verwerkingsverantwoordelijke worden Verwerkt zich ertoe verbindt de vertrouwelijkheid en de beveiliging van de Persoonsgegevens te waarborgen.

5 SUBVERWERKERS

5.1 Verwerkingsverantwoordelijke geeft Verwerker hierbij toestemming om gebruik te maken van Subverwerkers. Verwerker zal Verwerkingsverantwoordelijke op verzoek een lijst van de Subverwerkers verstrekken. Verwerker is gerechtigd om die lijst aan te passen en/of aan te vullen. Verwerker blijft verantwoordelijk voor de naleving van de Overeenkomst en de Verwerkersovereenkomst.

6 BEVEILIGING

6.1 Verwerker zal zich inspannen om geschikte administratieve, organisatorische, fysieke en technische maatregelen te treffen om de vertrouwelijkheid, integriteit en beschikbaarheid van de Persoonsgegevens te waarborgen in overeenstemming met de Gegevensbeschermingswetgeving en toepasselijke zorgwetgeving, waaronder maar niet uitsluitend, de bescherming van de Persoonsgegevens tegen vernietiging, hetzij per ongeluk, hetzij onrechtmatig, tegen verlies, niet-toegelaten verspreiding of toegang, dan wel tegen enige andere vorm van onrechtmatige verwerking. De Verwerker houdt rekening met de stand van de techniek en de implementatiekosten wanneer zij overweegt of dergelijke waarborgen passend zijn, en zorgt ervoor dat dergelijke maatregelen een passend beveiligingsniveau bieden, gelet op de risico's die de Verwerking en de aard van de te beschermen Persoonsgegevens met zich brengen.

6.2 **Bijlage 2** (Technische- en organisatorische maatregelen) beschrijft de maatregelen die Verwerker zal treffen en Verwerkersverantwoordelijke acht die maatregelen adequaat. Verwerker kan de Beveiligingsmaatregelen vermeld in Bijlage 2 periodiek updaten of wijzigen, voor zover dergelijke wijzigingen niet leiden tot een materiele verslechtering van het beveiligingsniveau. Verwerker streeft er naar Verwerkingsverantwoordelijke zo spoedig mogelijk op de hoogte stellen van de updates of wijzigingen.

7 VERZOEKEN VAN BETROKKENEN

7.1 Verwerker zal, voor zover redelijk en rekening houdend met de aard van de Verwerking, Verwerkingsverantwoordelijke bijstaan bij het nemen van geschikte technische en organisatorische maatregelen om de Verwerkingsverantwoordelijke in staat te stellen te voldoen aan de rechten van Betrokkenen zoals bedoeld in de Gegevensbeschermingswetgeving, waaronder het recht van toegang, het recht op rectificatie, het recht van gegevenswissing, het recht van beperking van de verwerking, het recht op dataportabiliteit, het recht van bezwaar en het recht om niet onderworpen te worden aan geautomatiseerde besluitvorming.

7.2 Verwerker reageert niet zelfstandig op verzoeken, klachten of vragen van personen (met inbegrip van, maar niet beperkt tot de Betrokkenen), behalve wanneer de wet zulks vereist. Verwerker zal na ontvangst naar eigen keuze (i) redelijke inspanningen verrichten om de Betrokkene door te verwijzen naar Verwerkingsverantwoordelijke om het verzoek of de klacht of vraag in te dienen of (ii) redelijke

inspanningen verrichten om het verzoek, de klacht of vraag door te sturen naar Verwerkingsverantwoordelijke. Verwerkingsverantwoordelijke is verantwoordelijk voor het beantwoorden van een verzoeken, klachten en vragen van Betrokkenen.

7.3 Verwerker is gerechtigd de Verwerkingsverantwoordelijke voor deze werkzaamheden kosten in rekening te brengen.

8 DATALEKKEN

8.1 Verwerker stelt Verwerkingsverantwoordelijke binnen 48 uur in kennis van elke feitelijke of redelijkerwijs vermoede accidentele of onwettige vernietiging, verlies, wijziging, ongeoorloofde bekendmaking van of toegang tot doorgezonden, opgeslagen of anderszins Verwerkte Persoonsgegevens (een "**Datalek**"), ongeacht of dit Datalek plaatsvindt bij de Verwerker.

8.2 Op verzoek en kosten van Verwerkingsverantwoordelijke verleent Verwerker alle redelijkerwijs vereiste medewerking in het afhandelen van een Datalek. Verwerker zal, zonder voorafgaande toestemming van Verwerkingsverantwoordelijke, geen mededeling doen aan Betrokkenen, Toezichthoudende Autoriteiten, regelgevende instellingen, handhavingsinstanties of elke andere derde partij, tenzij Verwerker wettelijk verplicht is een dergelijke mededeling te doen.

9 DOORGIFTE VAN PERSOONSGEGEVENS

9.1 Verwerker zal Persoonsgegevens uitsluitend verwerken in de EER.

10 TERMIJN, BEËINDIGING EN SCHORSING

10.1 Deze Verwerkersovereenkomst vormt een integraal onderdeel van de Overeenkomst. Deze Verwerkersovereenkomst treedt in werking op de datum van inwerkingtreding van de Overeenkomst en wordt automatisch beëindigd bij afloop of beëindiging van de Overeenkomst om welke reden dan ook.

10.2 Indien een partij een van haar verplichtingen uit hoofde van deze Verwerkersovereenkomst niet nakomt of niet in staat is de Verwerkersovereenkomst na te leven, kan de andere partij, onverminderd haar rechten op grond van de wet, de Overeenkomst of de Verwerkersovereenkomst, de Verwerking van Persoonsgegevens geheel of gedeeltelijk opschorten, totdat (i) de niet-nakoming is hersteld of weer wordt nagekomen; of (ii) de Overeenkomst en/of Verwerkersovereenkomst wordt beëindigt.

10.3 Onverminderd haar rechten op grond van de wet of de Overeenkomst, kan elke partij de Overeenkomst, met inbegrip van de Verwerkersovereenkomst, geheel of gedeeltelijk ontbinden indien de andere partij de Verwerking van Persoonsgegevens heeft opgeschort in overeenstemming met artikel 10.2 en binnen een redelijke termijn en in elk geval binnen twee (2) maanden na opschorting (i) de niet-nakoming niet hersteld is dan wel (ii) nakoming blijvend onmogelijk is.

11 RETOURNEREN OF WISSEN PERSOONSGEGEVENS

11.1 Bij beëindiging of afloop van deze Overeenkomst zal Verwerker, op schriftelijk verzoek van Verwerkingsverantwoordelijke, de Persoonsgegevens retourneren en/of verwijderen, behalve wanneer Verwerker op grond van de Overeenkomst, een wet, voorschrift of overheids- of regelgevende instantie verplicht is Persoonsgegevens te bewaren.

12 AUDIT

12.1 Verwerker verstrekt, op verzoek van Verwerkingsverantwoordelijke, de informatie die vereist is om te verifiëren dat Verwerker haar verplichtingen uit deze Verwerkersovereenkomst nakomt.

12.2 Verwerker onderwerpt haar Verwerkingsactiviteiten, op schriftelijk verzoek van Verwerkingsverantwoordelijke, aan een audit, uitgevoerd door een bevoegde onafhankelijke EDP-auditor. In een dergelijk geval zal Verwerkingsverantwoordelijke:

i. Verwerker binnen een redelijke termijn in kennis te stellen van het voornemen om een audit uit te voeren of te laten uitvoeren;

ii. zorg dragen voor de uitvoering van de audit met inachtneming van de redelijke vertrouwelijkheidseisen en zakelijke vereisten van de Verwerker; en

iii. zich redelijkerwijs inspannen om verstoring van de activiteiten van de Verwerker door de uitvoering van de audit tot een minimum te beperken.

12.3 De kosten van een audit worden gedragen door Verwerkingsverantwoordelijke.

12.4 De uitkomsten van de audit zullen door partijen in onderling overleg worden beoordeeld en, waar nodig, zullen partijen adequate maatregelen nemen

13 GARANTIES

13.1 partijen garanderen en verklaren dat zij:

(i) bij de uitvoering van de verplichtingen uit de Overeenkomst de Gegevensbeschermingswetgeving in acht nemen; en

(ii) geen reden hebben om te veronderstellen dat de Gegevensbeschermingswetgeving hen belet een van de in de Overeenkomst omschreven diensten te verlenen.

13.2 Verwerkingsverantwoordelijke garandeert dat:

(i) alle Persoonsgegevens die in het kader van deze Verwerkersovereenkomst aan Verwerker worden verstrekt, worden verzameld in overeenstemming met de Gegevensbeschermingswetgeving.

14 AANSPRAKELIJKHEID

14.1 Artikel 7 van de Algemene Voorwaarden is van toepassing.

15 MELDINGEN

15.1 Elke kennisgeving of andere mededeling aan een partij op grond van of in verband met deze Overeenkomst moet schriftelijk geschieden en worden gericht aan de contactpersoon zoals opgenomen op het Order Formulier.

16 TOEPASSELIJKE RECHT

16.1 Artikel 9 van de Algemene Voorwaarden is van toepasing.

BIJLAGE 1 – Betrokkenen en Categorieën van Persoonsgegevens

Soort persoonsgegevens	Betrokkenen
- NAW gegevens, geboortedatum, geslacht, bsn, telefoonnummer, e-mail - Verwijzingsgegevens van behandelaar, - Verzekeringsgegevens, - Behandelgegevens; behandeldata, tijdstip, behandelend therapeut, locatie, ruimte, verrichtingen, declaratiegegevens - EPD dossiergegevens, aanmelding gegevens, anamnese, onderzoek, behandelplan, dagjournalen, klinimetrie en vastgestelde meetwaarden van klinimetrie, tussen en eindrapportages	Cliënten / Patiënten van Verwerkingsverantwoordelijke

BIJLAGE 2 – Technische- en organisatorische maatregelen

Verwerker heeft een functionerend en actief Information Security Management System (ISMS) dat is ingericht volgens de ISO/IEC 27001 en NEN 7510 normen. Verwerker is hiervoor officieel gecertificeerd en wordt jaarlijks door een externe partij aan een audit onderworpen.

Maatregelen om de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van verwerkingssystemen en -diensten te waarborgen;
Cryptography, conform ISO27001; waarin onder andere is vastgelegd dat data wordt versleuteld om vertrouwelijkheid te borgen. Hiervoor worden door Verweker minimaal de "Near term protection" en bij voorkeur de "Long-term protection" aanbevelingen aangehouden van de ECRYPT-CSA aanbevelingen.

Maatregelen om ervoor te zorgen dat de beschikbaarheid van, en toegang tot persoonsgegevens tijdig kunnen worden hersteld in geval van een fysiek of technisch incident;
Herstel van gegevens conform ISO27001, waarin de kaders van backupmethodiek, frequentie en herstelprocedure zijn vastgelegd. Hier vallen ook zaken als retentie, recovery en encryptie onder. Backups worden periodiek getest als validatie. De resultaten van deze test worden vastgelegd in het daarvoor bestemde systeem.

Processen voor het regelmatig testen, beoordelen en evalueren van de effectiviteit van technische en organisatorische maatregelen om de veiligheid van de verwerking te waarborgen;

Conform ISO 27001 / NEN 7510 vervult Verwerker periodiek zowel interne als externe audits om vast te stellen dat het Information Security Management System (ISMS) naar behoren functioneert.

Maatregelen voor gebruikersidentificatie en -autorisatie;
Identificatie en autorisatie conform ISO27001. Dit omvat onder andere principes zoals 'least privilege' en 'need to know' permissiebeleid.

Maatregelen voor de bescherming van gegevens tijdens de opslag;
Zie cryptografische maatregelen voor gegevensbescherming hierboven.

Maatregelen voor het waarborgen van logboekregistratie van gebeurtenissen en logboekanalyse;
Verwerker heeft beleid en implementatie omtrent logging ingericht conform ISO27001. Dit omvat zowel auditlogging van toegang tot de cloudomgeving, maar ook wat er binnen de cloudomgeving gebeurt. Loggegevens worden beschermd tegen verwijdering en manipulatie. Logboekanalyse vindt periodiek plaatst en de resultaten van deze test worden vastgelegd in het daarvoor bestemde systeem.

Maatregelen om een veilige systeemconfiguratie te waarborgen;
Conform ISO27001 heeft Verwerker maatregelen getroffen voor veilige softwareontwikkeling en operationele processen, waaronder systeemconfiguratie. Samengevat heeft Verwerker een functionerende OTAP-straat waarbij configuraties en programmacode in revisiebeheersoftware worden vastgelegd en vervolgens door de OTAP gaat.

Maatregelen voor certificering/borging van processen;
Verwerker committeert zich aan diverse certificeringen en is momenteel gecertificeerd voor ISO27001 en NEN7510.

Maatregelen om de kwaliteit van de gegevens te waarborgen;
Technisch: Beheersmaatregelen voor opslag van data (d.w.z. statische data).
Organisatorisch: Verwerker heeft dit proces geïmplementeerd en gedocumenteerd.

Maatregelen om de verantwoordingsplicht te waarborgen;
Verwerker heeft een functionerend Information Security Management System die de verantwoordingsplicht borgt. Zowel organisatorisch als technisch door periodieke certificeringen: ISO27001 en NEN7510. Het voorziet in het toekomstig kunnen continueren van deze plicht conform ISO27001 Annex A.17.1 - Information security continuity. Periodieke verificatie vindt plaats conform ISO27001 Annex A.17.1.3 - Verify, review and evaluate information security continuity.