

## Verwerkersovereenkomst

### DE ONDERGETEKENDEN:

Marks Fysiotherapie gevestigd aan Kapelstraat 84, 5751 CG te Beek en Donk en ingeschreven in het register van de Kamer van Koophandel onder nummer 17255942, in deze rechtsgeldig vertegenwoordigd door K. Marks, Fysiotherapeut (hierna: “Verwerkingsverantwoordelijke”)

en

ENOVATION B.V, h.o.d.n. VANAD Enovation, gevestigd aan de Rivium Westlaan 1, 2909 LD te Capelle aan den IJssel en ingeschreven in het register van de Kamer van Koophandel onder nummer 24157738, in deze rechtsgeldig vertegenwoordigd door J.O. van Rijswijk, CEO hierna (“Verwerker”).

### Overwegende dat

- a Verwerker diensten verricht ten behoeve van Verwerkingsverantwoordelijke, zoals beschreven in de Hoofdovereenkomst met referentie 500053442 ten behoeve van ZorgMail.
- b De diensten met zich meebrengen dat persoonsgegevens worden verwerkt, waaronder gegevens betreffende de gezondheid.
- c Verwerker de betreffende gegevens louter in opdracht van Verwerkingsverantwoordelijke verwerkt en niet voor eigen doeleinden.
- d Per 25 mei 2018 van toepassing zal zijn Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 (Algemene Verordening Gegevensbescherming).
- e Partijen middels deze Verwerkersovereenkomst de afspraken met betrekking tot de verwerking van persoonsgegevens in het kader van de diensten wensen vast te leggen.
- f Deze Verwerkersovereenkomst, indien van toepassing, alle eerdere overeenkomst(en) van gelijke strekking tussen Partijen vervangt.

### Definities

In deze Verwerkersovereenkomst wordt onder de volgende met een hoofdletter aangeduide begrippen het volgende verstaan:

- |    |  |   |
|----|--|---|
| a) | Algemene Verordening Gegevens Bescherming of AVG | Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG. |
| b) | Betrokkene                                       | een geïdentificeerde of identificeerbare natuurlijke persoon (artikel 4 sub 1 AVG).   |

- c) Derde een derde als bedoeld in artikel 4 sub 10 AVG.
- d) Functionaris voor de Gegevensbescherming een functionaris als bedoeld in artikel 37 e.v. AVG.
- e) Incident
  - i een klacht of (informatie)verzoek van een Betrokkene met betrekking tot de verwerking van Persoonsgegevens door Verwerker;
  - ii een onderzoek naar of beslaglegging door overheidsfunctionarissen op de Persoonsgegevens of een vermoeden dat dit gaat plaatsvinden;
  - iii een inbreuk in verband met Persoonsgegevens als bedoeld in artikel 4 onder 12 AVG;
  - iv iedere ongeautoriseerde toegang, verwijdering, verminking, verlies of enige andere vorm van onrechtmatige verwerking van de Persoonsgegevens.
- f) Medewerker de door Partijen voor de uitvoering van deze Verwerkersovereenkomst betrokken natuurlijke persoon die werkzaam is bij of voor een van de Partijen.
- g) Hoofdovereenkomst(en) de overeenkomst(en) betreffende de levering van producten en/of diensten.
- h) Partij Verwerkingsverantwoordelijke of Verwerker.
- i) Partijen Verwerkingsverantwoordelijke en Verwerker.
- j) Persoonsgegeven alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon in de zin van artikel 4 onder 1 AVG.
- k) Subverwerker iedere niet-ondergeschikte derde partij die door Verwerker is betrokken bij de verwerking van Persoonsgegevens in het kader van de Overeenkomst, niet zijnde Medewerkers.
- l) Verwerker de verwerker als bedoeld in artikel 4 sub 8 AVG.
- m) Verwerkersovereenkomst de onderhavige overeenkomst.
- n) Verwerkingsverantwoordelijke de verwerkingsverantwoordelijke als bedoeld in artikel 4 sub 7 AVG.
- o) Wet bescherming persoonsgegevens of Wbp Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens), inclusief latere wijzigingen.

## VERKLAREN TE ZIJN OVEREENGEKOMEN ALS VOLGT:

### Artikel 1. Definities

- 1.1 Voor zover begrippen met een hoofdletter niet afzonderlijk gedefinieerd zijn in deze Verwerkersovereenkomst, gelden in deze Verwerkersovereenkomst de definities zoals genoemd in de Hoofdovereenkomst, zijnde de overeenkomst als genoemd in overweging (a) en de toepasselijke voorwaarden.
- 1.2 Genoemde en overige begrippen worden geïnterpreteerd overeenkomstig de AVG. Tot aan 25 mei 2018 worden begrippen geïnterpreteerd overeenkomstig de vergelijkbare bepaling uit de Wbp.
- 1.3 Waar in deze Verwerkersovereenkomst naar bepaalde normen wordt verwezen (zoals NEN7510) wordt daarmee steeds bedoeld op de meest actuele versie daarvan. Voor zover de betreffende norm niet meer wordt onderhouden, dient in de plaats daarvan de meest actuele versie van de logische opvolger van de betreffende norm gelezen te worden.

### Artikel 2. Onderwerp van deze Verwerkersovereenkomst

- 2.1 Verwerker verwerkt in opdracht van Verwerkingsverantwoordelijke gedurende de looptijd van de in artikel 1 van deze Verwerkersovereenkomst genoemde Hoofdovereenkomst ten behoeve van Verwerkingsverantwoordelijke en ter voldoening aan enige wettelijke verplichting persoonsgegevens. Een overzicht van de categorieën Persoonsgegevens en de doeleinden waarvoor de persoonsgegevens ten behoeve van Verwerkingsverantwoordelijke worden verwerkt is opgenomen in Annex 1 bij deze Verwerkersovereenkomst.

### Artikel 3. Uitvoering verwerking

- 3.1 Verwerker garandeert dat hij ten behoeve van Verwerkingsverantwoordelijke uitsluitend persoonsgegevens zal verwerken voor zover dit noodzakelijk is voor de levering van de prestaties onder de in artikel 1 van deze Verwerkersovereenkomst genoemde Hoofdovereenkomst. Overige verwerkingen zullen uitsluitend worden uitgevoerd in expliciete opdracht van Verwerkingsverantwoordelijke of als daartoe een wettelijke verplichting bestaat na informeren van Verwerkingsverantwoordelijke. Informeren van Verwerkingsverantwoordelijke blijft achterwege waar dat in strijd zou zijn met de wet. In geen geval zal Verwerker persoonsgegevens verwerken voor eigen doeleinden.
- 3.2 Verwerker zal alle redelijke verzoeken van Verwerkingsverantwoordelijke in verband met de verwerking van de persoonsgegevens opvolgen. Verwerker stelt Verwerkingsverantwoordelijke onmiddellijk op de hoogte indien naar zijn oordeel instructies in strijd zijn met de toepasselijke wetgeving met betrekking tot de verwerking van persoonsgegevens.
- 3.3 Verwerker zal de Persoonsgegevens aantoonbaar, op behoorlijke en zorgvuldige wijze verwerken en in overeenstemming met de op hem als Verwerker rustende verplichtingen op grond van de AVG, voor zover nog van toepassing de Wbp, en overige wet- en regelgeving. Verwerker zal in dat kader ten minste een register van verwerkingen aanleggen als bedoeld in artikel 30 AVG. Verwerker is gehouden om, met inachtneming van hetgeen in deze Verwerkersovereenkomst is bepaald, die doeleinden en de bescherming van de persoonsgegevens met maximale zorg na te streven.

- 3.4 Verwerker zal, tenzij hij hiervoor uitdrukkelijke voorafgaande schriftelijke toestemming heeft verkregen van Verwerkingsverantwoordelijke, geen persoonsgegevens verwerken of laten verwerken door hemzelf of door derden in landen buiten de Europese Economische Ruimte ("EER") zonder een passend beschermingsniveau. Verwerker stelt de in Annex 3 genoemde medewerker van Verwerkingsverantwoordelijke onmiddellijk schriftelijk op de hoogte van alle (geplande) permanente of tijdelijke doorgiften van persoonsgegevens naar een land buiten de Europese Economische Ruimte. Verwerker zal pas uitvoering geven aan dergelijke (geplande) doorgiften na schriftelijke toestemming van Verwerkingsverantwoordelijke. Verwerkingsverantwoordelijke heeft te allen tijde het recht om aanvullende voorwaarden te verbinden aan haar toestemming voor een dergelijke verwerking.
- 3.5 Verwerker zal Verwerkingsverantwoordelijke informeren over iedere wijziging van de locatie waar de gegevens van Verwerkingsverantwoordelijke worden opgeslagen, evenals over de identiteit van eventuele derde partijen die hierbij betrokken zijn.
- 3.6 Verwerker garandeert dat hij alle persoonsgegevens als strikt vertrouwelijk zal behandelen en dat hij al zijn werknemers, vertegenwoordigers en/of onderaannemers die betrokken zijn bij de verwerking van de Persoonsgegevens van de vertrouwelijke aard van dergelijke (persoons)gegevens op de hoogte zal stellen. Verwerker zal waarborgen dat betrokken personen en partijen een geheimhoudingsovereenkomst hebben getekend. Het is Verwerker niet toegestaan de persoonsgegevens aan enige derde te tonen, te verstrekken of anderszins ter beschikking te stellen, tenzij dit noodzakelijk of toegestaan is ingevolge de opdracht van de in lid 1 genoemde Hoofdovereenkomst of in het geval hiervoor expliciete voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke is verkregen.
- 3.7 Verwerker zal, binnen zijn invloedssfeer, zijn volledige en tijdige medewerking verlenen aan Verwerkingsverantwoordelijke om (i) na goedkeuring van en in opdracht van Verwerkingsverantwoordelijke betrokkenen toegang te laten krijgen tot de hun betreffende persoonsgegevens, (ii) persoonsgegevens te verwijderen of te corrigeren, (iii) aan te tonen dat persoonsgegevens verwijderd of gecorrigeerd zijn indien zij incorrect zijn (of, ingeval Verwerkingsverantwoordelijke het er niet mee eens is dat persoonsgegevens incorrect zijn, het feit vast te leggen dat de betrokkene zijn persoonsgegevens als incorrect beschouwt) en (iv) Verwerkingsverantwoordelijke anderszins in de gelegenheid te stellen om aan zijn verplichtingen onder de Wbp of andere toepasselijke wetgeving op het gebied van verwerking van persoonsgegevens te voldoen.
- 3.8 Verwerker zal de persoonsgegevens van Verwerkingsverantwoordelijke logisch gescheiden verwerken van de persoonsgegevens die hij voor zichzelf of namens derde partijen verwerkt.
- 3.9 Onverminderd het bepaalde in het eerste lid van dit artikel 3, is het Verwerker toegestaan om Persoonsgegevens te verwerken indien een wettelijk voorschrift (waaronder begrepen daarop gebaseerde rechterlijke of bestuurlijke bevelen) hem tot een verwerking verplicht. In dat geval stelt Verwerker voorafgaand aan de verwerking Verwerkingsverantwoordelijke in kennis van de beoogde verwerking en het wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt. Verwerker zal Verwerkingsverantwoordelijke, waar mogelijk, in staat stellen zich te verweren tegen deze verplichte verwerking en ook overigens de verplichte verwerking beperken tot het strikt noodzakelijke.

- 3.10 Voor zover de (verzameling van) Persoonsgegevens wordt beschermd door enig intellectueel eigendomsrecht, verleent Verwerkingsverantwoordelijke toestemming aan Verwerker de Persoonsgegevens te gebruiken in het kader van de uitvoering van deze Verwerkersovereenkomst.

#### **Artikel 4. Beveiliging persoonsgegevens & controle**

- 4.1 Verwerker zal passende technische en organisatorische beveiligingsmaatregelen nemen, die gezien de huidige stand der techniek en de daarmee gemoeide kosten overeenstemmen met de aard van de te verwerken persoonsgegevens, ter bescherming van de persoonsgegevens tegen verlies, onbevoegde kennisname, verminking of onrechtmatige verwerking, alsmede om de (tijdige) beschikbaarheid van de gegevens te garanderen. In deze beveiligings- maatregelen zijn de mogelijk in de Hoofdovereenkomst reeds bepaalde maatregelen begrepen. De maatregelen omvatten in ieder geval:
- (a) maatregelen om te waarborgen dat enkel bevoegde Medewerkers toegang hebben tot de Persoonsgegevens voor de doeleinden die zijn uiteengezet;
  - (b) maatregelen waarbij Verwerker zijn medewerkers en Subverwerkers uitsluitend toegang geeft tot persoonsgegevens via op naam gestelde accounts, waarbij het gebruik van die accounts adequaat gelogd wordt en waarbij de betreffende accounts alleen toegang geven tot die persoonsgegevens waartoe de toegang voor de betreffende (rechts)persoon noodzakelijk is;
  - (c) maatregelen om de Persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, onopzettelijk verlies of wijziging, onbevoegde of onrechtmatige opslag verwerking, toegang of openbaarmaking;
  - (d) maatregelen om zwakke plekken te identificeren ten aanzien van de verwerking van persoonsgegevens in de systemen die worden ingezet voor het verlenen van diensten aan Verwerkingsverantwoordelijke;
  - (e) maatregelen om de tijdige beschikbaarheid van de gegevens te garanderen,
  - (f) de overige maatregelen die Partijen in Annex 2 en in de Hoofdovereenkomst zijn overeengekomen.
- 4.2 Verwerker werkt aantoonbaar in overeenstemming met ISO27001 en/of NEN 7510 en heeft een passend, geschreven beveiligingsbeleid geïmplementeerd voor de verwerking van persoonsgegevens, waarin in ieder geval de in lid 1 van dit artikel 4 genoemde maatregelen uiteen zijn gezet.
- 4.3 Verwerker voldoet aan de eisen van andere NEN-normen voor zover die voor de gezondheidszorg van toepassing zijn verklaard.
- 4.4 Verwerkingsverantwoordelijke heeft het recht toe te laten zien door een deskundige, onafhankelijke, derde partij op de naleving van de hiervoor onder 4.1 t/m 4.3 genoemde maatregelen. Verwerker stelt Verwerkingsverantwoordelijke, indien Verwerkingsverantwoordelijke daarom verzoekt, hiertoe maximaal éénmaal per jaar in de gelegenheid op een door Partijen in gezamenlijk overleg nader te bepalen tijdstip en verder indien Verwerkingsverantwoordelijke daar aanleiding toe ziet naar aanleiding van (vermoeden van) informatie- of privacy-incidenten, zulks te laten controleren. Verwerker zal eventuele door Verwerkingsverantwoordelijke naar aanleiding van een dergelijke controle in redelijkheid gegeven instructies tot aanpassing van het beveiligingsbeleid binnen een redelijke termijn opvolgen.
- 4.5 Verwerker zal in alle redelijkheid haar medewerking verlenen aan het onder 4.4 hiervoor bedoelde onderzoek.

- 4.6 Partijen erkennen dat beveiligingseisen voortdurend veranderen en dat een effectieve beveiliging frequente evaluatie en regelmatige verbetering van verouderde beveiligingsmaatregelen vereist. Partijen zullen daarom de maatregelen zoals geïmplementeerd op basis van dit artikel 4 periodiek evalueren. Maatregelen worden in goed overleg tussen Partijen en verscherpt, aangevuld of verbeterend om te blijven voldoen aan de verplichtingen onder dit artikel 4.
- 4.7 Kosten, voortvloeiende uit het onderzoek als bedoeld onder artikel 4.4, zijn voor rekening van Verwerkingsverantwoordelijke, tenzij de aanpassingen noodzakelijk zijn voor de naleving van verplichtingen als gesteld in deze Verwerkersovereenkomst.

### **Artikel 5. Monitoring, informatieplichten en incidentenmanagement**

- 5.1 Verwerker zal actief monitoren op inbreuken op de beveiligingsmaatregelen en over de resultaten van de monitoring in overeenstemming met dit artikel 5 rapporteren aan Verwerkingsverantwoordelijke.
- 5.2 Zodra zich een Incident met betrekking tot de verwerking van de persoonsgegevens voordoet, heeft voorgedaan of zou kunnen voordoen, is Verwerker verplicht Verwerkingsverantwoordelijke daarvan ogenblikkelijk, doch binnen 48 uur, in kennis te stellen en daarbij alle relevante informatie te verstrekken omtrent (1) de aard en omvang van het Incident, (2) de (mogelijk) getroffen gegevens, (3) de geconstateerde en de vermoedelijke gevolgen van het Incident, en (4) de maatregelen die getroffen zijn of zullen worden om het incident op te lossen dan wel de gevolgen/schade zoveel mogelijk te beperken.
- 5.3 Verwerker is, onverminderd de overige verplichtingen uit dit artikel, verplicht om maatregelen te treffen die redelijkerwijs van hem kunnen worden verwacht om het Incident zo snel mogelijk te herstellen dan wel de verdere gevolgen zoveel mogelijk te beperken. Verwerker treedt onverwijld in overleg met Verwerkingsverantwoordelijke teneinde hierover nadere afspraken te maken.
- 5.4 Verwerker zal Verwerkingsverantwoordelijke te allen tijde zijn medewerking verlenen en zal de redelijke verzoeken van Verwerkingsverantwoordelijke opvolgen, met als doel Verwerkingsverantwoordelijke in staat te stellen een deugdelijk onderzoek te verrichten naar het Incident, een correcte respons te formuleren en passende vervolgstappen te nemen ten aanzien van het Incident, waaronder begrepen het mogelijk informeren van de Autoriteit Persoonsgegevens (AP) en/of de betrokkene zoals bepaald in artikel 5.7.
- 5.5 Verwerker zal te allen tijde geschreven procedures voorhanden hebben die hem in staat stellen om Verwerkingsverantwoordelijke van een onmiddellijke reactie over een Incident te voorzien, en om effectief samen te werken met Verwerkingsverantwoordelijke om het Incident af te handelen.
- 5.6 Meldingen die worden gedaan op grond van dit artikel worden ogenblikkelijk gericht aan de in Annex 3 opgenomen Medewerker(s) van Verwerkingsverantwoordelijke of, indien relevant, aan een andere door Verwerkingsverantwoordelijke tijdens de duur van deze Verwerkersovereenkomst schriftelijk bekendgemaakte andere Medewerker van Verwerkingsverantwoordelijke.
- 5.7 Verwerkingsverantwoordelijke zal, indien naar zijn oordeel noodzakelijk, betrokkenen en andere derden w.o. de AP informeren over incidenten. Het is Verwerker niet toegestaan informatie te verstrekken over incidenten aan betrokkenen of andere derde partijen, behoudens voor zover Verwerker daartoe wettelijk verplicht is.
- 5.8 In concrete gevallen, en altijd na overleg met Verwerkingsverantwoordelijke, kan het mogelijk zijn dat Verwerker de eerste melding van een incident aan de AP doet. Over

deze melding en over de voortgang daarvan, houdt Verwerker Verwerkingsverantwoordelijke voortdurend op de hoogte.

### **Artikel 6. Gebruik onderaannemers**

- 6.1 Verwerker zal zijn activiteiten die (deels) bestaan uit het verwerken van persoonsgegevens of vereisen dat persoonsgegevens verwerkt worden niet uitbesteden aan een derde partij zonder voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke. Deze toestemming zal niet zonder redelijke grond worden geweigerd.
- 6.1.a Indien Verwerker besluit zijn activiteiten uit te besteden aan een vervangende derde partij en daarbij minimaal dezelfde danwel strengere eisen oplegt dan aan de – momenteel - ingeschakelde derde partij. Met inachtneming van artikel 6.1. zal toestemming niet worden geweigerd door Verwerkingsverantwoordelijke.
- 6.2 Verwerker zal aan de door hem ingeschakelde derde dezelfde of strengere verplichtingen opleggen als voor hemzelf uit deze Verwerkersovereenkomst en de wet voortvloeien en ziet toe op de naleving daarvan door de derde partij. De betreffende afspraken met de derde partij zullen schriftelijk worden vastgelegd.
- 6.3 Niettegenstaande de toestemming van Verwerkingsverantwoordelijke voor het inschakelen van een derde partij blijft Verwerker volledig aansprakelijk jegens Verwerkingsverantwoordelijke voor de gevolgen van het uitbesteden van werkzaamheden aan een derde. De toestemming van Verwerkingsverantwoordelijke voor het uitbesteden van werkzaamheden aan een derde partij laat onverlet dat voor de inzet van sub verwerkers in een land buiten de Europese Economische Ruimte zonder een passend beschermingsniveau toestemming vereist is in overeenstemming met artikel 3.4 van deze Verwerkersovereenkomst.

### **Artikel 7. Aansprakelijkheid**

- 7.1 Partijen zijn ieder verantwoordelijk en aansprakelijk voor hun eigen handelen. De aansprakelijkheid van Verwerker voor directe schade als gevolg van een toerekenbare tekortkoming in de nakoming van de Verwerkersovereenkomst, dan wel uit onrechtmatige daad of anderszins, is per gebeurtenis (een reeks van opeenvolgende gebeurtenissen geldt als één gebeurtenis) beperkt tot de vergoeding van directe schade, tot maximaal een bedrag dat ten tijde van de tekortkoming waren gefactureerd of hadden kunnen worden gefactureerd in de voorgaande 12 maanden. De aansprakelijkheid van Verwerker voor directe schade zal in totaal nooit meer bedragen dan EUR 10.000,00 (zegge : tienduizend).
- 7.2 Onder directe schade wordt verstaan:  
Schade aan programmatuur en gegevensbestanden, waaronder in elk geval verstaan wordt:
  - a) Materiële beschadiging, gebrekkig of niet functioneren, verminderde betrouwbaarheid en verhoogde storingsgevoeligheid;
  - b) Schade aan andere eigendommen van Verwerkingsverantwoordelijke en/of van derden;
  - c) Kosten van noodzakelijke wijzigingen en/of veranderingen in programmatuur, specificaties, materialen of documentatie, aangebracht ter beperking c.q. herstel van schade;
  - d) De kosten van noodvoorzieningen, zoals het uitwijken naar andere computersystemen, het inhuren van derden of het hanteren van noodprocedures of afwijkende werkwijzen;

- e) Kosten, waaronder begrepen personeelskosten, van het noodgedwongen langer operationeel houden van (het) oude syste(m)en en daarmee samenhangende voorzieningen;
  - f) De kosten van leegloop van medewerkers, goederen en faciliteiten van Verwerkingsverantwoordelijke en de kosten van leegloop van door Verwerkingsverantwoordelijke in het kader van de uitvoering van de Overeenkomst ingehuurd derden, voor zover deze kosten, in redelijkheid, niet vermijdbaar zijn;
  - g) Redelijke kosten gemaakt ter voorkoming of beperking van directe schade, die als gevolg van de gebeurtenis waarop de aansprakelijkheid berust, mocht worden verwacht;
  - h) Redelijke kosten gemaakt ter vaststelling van de schade-oorzaak, de aansprakelijkheid, de directe schade en de wijze van herstel.
  - i) Boetes en dwangsommen als opgelegd door de Autoriteit Persoonsgegevens – voor dit lid vervalt de limitering als bedoeld in art. 7.1.
- 7.3 De aansprakelijkheid van Verwerker voor indirecte schade is uitgesloten. Onder indirecte schade wordt verstaan alle schade die geen directe schade is en daarmee in ieder geval, maar niet beperkt tot, gevolgschade, gederfde winst, gemiste besparingen, verminderde goodwill, schade door bedrijfsstagnatie, schade door het niet behalen van marketingdoeleinden, schade verband houdende met het gebruik door Verantwoordelijke voorgeschreven gegevens of databestanden, of verlies, vermindering of vernietiging van gegevens of databestanden, voor zover niet bedoeld als genoemd in artikel 7.2.a.
- 7.4 De in dit artikel bedoelde uitsluitingen en beperkingen komen te vervallen indien en voor zover de schade het gevolg is van opzet of bewuste roekeloosheid van Verwerker of haar bedrijfsleiding.
- 7.5 Tenzij nakoming door Verwerker blijvend onmogelijk is, ontstaat de aansprakelijkheid van Verwerker wegens toerekenbare tekortkoming in de nakoming van de Verwerkersovereenkomst slechts indien Verwerkingsverantwoordelijke Verwerker onverwijld schriftelijk in gebreke stelt, waarbij een redelijke termijn voor herstel van de tekortkoming wordt gesteld, en Verwerker ook na die termijn toerekenbaar blijft tekortschieten in de nakoming van haar verplichtingen. De ingebrekestelling dient een zo volledig en gedetailleerd mogelijke omschrijving van de tekortkoming te bevatten, opdat Verwerker in de gelegenheid wordt gesteld adequaat te reageren.
- 7.6 Iedere vordering tot schadevergoeding door Verwerkingsverantwoordelijke tegen Verwerker die niet gespecificeerd en expliciet is gemeld, vervalt door het enkele verloop van twaalf (12) maanden na het ontstaan van de voor Verwerkingsverantwoordelijke redelijkerwijs kenbare vordering.
- 7.7 Verwerker zal zich gedurende de Verwerkersovereenkomst adequaat verzekerd hebben en houden conform dit artikel.

## **Artikel 8. Duur en beëindiging**

- 8.1 Deze Verwerkersovereenkomst gaat in op de datum van ondertekening en de duur van deze Verwerkersovereenkomst is gelijk aan de duur van de in artikel 1 genoemde Hoofdovereenkomst.
- 8.2 De Verwerkersovereenkomst maakt na ondertekening ervan door beide Partijen integraal en onlosmakelijk deel uit van de Hoofdovereenkomst. Beëindiging van de Hoofdovereenkomst, op welke grond dan ook (opzegging/ontbinding), heeft tot gevolg



- dat de Verwerkersovereenkomst eveneens op dezelfde grond beëindigd wordt (en vice versa), tenzij partijen in voorkomend geval anders overeenkomen.
- 8.3 Verplichtingen welke naar hun aard bestemd zijn om ook na beëindiging van deze Verwerkersovereenkomst voort te duren, blijven na beëindiging van deze Verwerkersovereenkomst gelden. Tot deze bepalingen behoren onder meer die welke voortvloeien uit de bepalingen betreffende geheimhouding, aansprakelijkheid en toepasselijk recht.
- 8.4 Ieder der partijen is gerechtigd, onverminderd hetgeen daartoe bepaald is in de Hoofdovereenkomst, de uitvoering van deze Verwerkersovereenkomst en de daarmee samenhangende Hoofdovereenkomst op te schorten, dan wel zonder rechterlijke tussenkomst met onmiddellijke ingang te ontbinden, indien:
- (a) de andere partij wordt ontbonden of anderszins ophoudt te bestaan;
  - (b) de andere partij aantoonbaar tekortschiet in de nakoming van de verplichtingen die voortvloeien uit deze Verwerkersovereenkomst en die ernstige toerekenbare tekortkoming niet binnen redelijke en in samenspraak vastgestelde termijn is hersteld na een daartoe strekkende schriftelijke ingebrekestelling;
  - (c) een partij in staat van faillissement wordt verklaard of surséance van betaling aanvraagt.
- 8.4 Verwerker informeert ogenblikkelijk Verwerkingsverantwoordelijke indien een faillissement dreigt dan wel surséance van betaling, zodat Verwerkingsverantwoordelijke tijdig kan beslissen de persoonsgegevens terug te vorderen alvorens faillissement wordt uitgesproken.
- 8.5 Verwerker dient Verwerkingsverantwoordelijke voorafgaand en tijdig te informeren over een voorgenomen overname of eigendomsoverdracht.
- 8.6 Verwerkingsverantwoordelijke is gerechtigd deze Verwerkersovereenkomst en de Hoofdovereenkomst per direct te ontbinden indien Verwerker te kennen geeft niet (langer) te kunnen voldoen aan de betrouwbaarheidseisen die op grond van ontwikkelingen in de wet en/of de rechtspraak aan de verwerking van de persoonsgegevens worden gesteld. Artikel 9.2 is van overeenkomstige toepassing.
- 8.7 Gelet op de grote afhankelijkheid van Verwerkingsverantwoordelijke van Verwerker alsmede het continuïteitsrisico bij incidenten en calamiteiten (zoals faillissement), verklaart Verwerker zich reeds nu voor alsdan bereid op eerste verzoek van Verwerkingsverantwoordelijke aanvullende afspraken met Verwerkingsverantwoordelijke te maken teneinde voornoemde risico's te verkleinen.

### **Artikel 9. Bewaartermijnen, teruggave en vernietiging van Persoonsgegevens**

- 9.1 Verwerker zal de Persoonsgegevens niet langer bewaren dan nodig is voor de in artikel 3.2 genoemde doelen. Verwerkingsverantwoordelijke zal waar de Persoonsgegevens niet meer nodig zijn Verwerkingsverantwoordelijke raadplegen ter zake de voortzetting van het bewaren van die Persoonsgegevens.
- 9.2 Bij beëindiging van de Verwerkersovereenkomst, of indien van toepassing aan het einde van de overeengekomen bewaartermijnen, of op schriftelijk verzoek van Verwerkingsverantwoordelijke zal Verwerker, kosteloos, naar keuze van Verwerkingsverantwoordelijke, de persoonsgegevens onherroepelijk vernietigen of teruggeven aan Verwerkingsverantwoordelijke. Op verzoek van Verwerkingsverantwoordelijke verstrekt Verwerker bewijs van het feit dat de gegevens onherroepelijk vernietigd of verwijderd zijn. Eventuele teruggave van de gegevens zal in een algemeen gangbaar, gestructureerd gegevensformaat langs elektronische weg


plaatsvinden. Indien teruggave, onherroepelijke vernietiging of verwijdering niet mogelijk zijn, stelt Verwerker Verwerkingsverantwoordelijke daarvan onmiddellijk op de hoogte. In dat geval garandeert Verwerker dat hij de persoonsgegevens vertrouwelijk zal behandelen en niet langer zal verwerken.

- 9.3 Bij het einde van de Verwerkersovereenkomst zal Verwerker alle onderaannemers die betrokken zijn bij het verwerken van persoonsgegevens op de hoogte stellen van de beëindiging van de Verwerkersovereenkomst. De verplichtingen uit artikel 9.2 zijn van overeenkomstige toepassing op deze onderaannemers, en Verwerker zal waarborgen dat alle betrokken onderaannemers hieraan uitvoering zullen geven.

## **Artikel 10. Slotbepalingen**

- 10.1 De overwegingen maken onderdeel uit van deze Verwerkersovereenkomst.
- 10.2 In het geval van strijdigheid tussen de bepalingen uit deze Verwerkersovereenkomst en bepalingen uit de in artikel 1 genoemde Hoofdovereenkomst zullen de bepalingen van de Verwerkersovereenkomst leidend zijn.
- 10.3 In geval van nietigheid c.q. vernietigbaarheid van een of meer bepalingen uit deze Verwerkersovereenkomst, blijven de overige bepalingen onverkort van kracht.
- 10.4 In alle gevallen waarin deze Verwerkersovereenkomst niet voorziet beslissen partijen in onderling overleg.
- 10.5 Op deze Verwerkersovereenkomst is louter Nederlands recht van toepassing.
- 10.6 Eventuele conflicten zullen eerst met elkaar besproken worden waarbij beide partijen zich inspannen om deze in goed overleg met elkaar op te lossen, daarin begrepen de mogelijkheid het geschil te beëindigen door een in onderling overleg vast te stellen mediation of arbitrage.
- 10.7 Geschillen over of in verband met deze Verwerkersovereenkomst worden uitsluitend voorgelegd aan de bevoegde rechter in het arrondissement van Verwerkingsverantwoordelijke.

Marks Fysiotherapie



K. Marks  
Fysiotherapeut

Plaats: Beek en Donk

Datum: 14-09-2018

ENOVATION B.V.



J.O. van Rijswijk  
CEO

Plaats: Capelle aan den IJssel

Datum: 14-09-2018

## **ANNEX 1: Te verwerken persoonsgegevens en doeleinden**

### Aard van de Verwerking

Verwerking patiënt- en cliëntgegevens

### Te verwerken persoonsgegevens

Persoonsgegevens die (kunnen) worden verwerkt op basis van de Hoofdovereenkomst

- Naam-, adres- en woonplaatsgegevens;
- Telefoonnummers;
- E-mailadressen of andere adressen voor elektronische communicatie;
- Burgerservicenummer (BSN) of sofinummer;
- Geslacht, geboortedatum, en/of leeftijd;
- Nationaliteit of geboorteplaats;
- Medische gegevens;
- Overige / onbekend.

### Doeleinden van de Verwerking

Verwerkingsverantwoordelijke

Zorg en welzijn

Individuele gezondheidszorg

- a. het uitoefenen van het beroep in de individuele gezondheidszorg, individueel of in samenwerkingsverband,
- b. het verlenen van zorg;

Verwerker

Uitvoeren van contractuele overeenkomst (dienstverlening zoals beschreven in Hoofdovereenkomst)

Middelen van verwerking :

ZorgMail

VANAD Enovation maakt voor haar hosting activiteiten tbv ZorgMail gebruik van een hosting partij. Deze partij is aangemerkt als sub verwerker en zal ten minste voldoen aan de vereisten van ISO27001 en NEN7510 en haar datacenters binnen de EU hebben ondergebracht.

**ANNEX 2: Beveiligingsmaatregelen**

Zie hiertoe de bijlage Informatiebeveiliging ZorgMail

**ANNEX 3: Contactgegevens**

Functionarissen waarmee contact dient te worden opgenomen in het geval van een datalek.

Primair aanspreekpunt  
Verwerkingsverantwoordelijke:

Fysiotherapeut
K. Marks
info@marksfysiotherapie.nl
(0492)464745

Primair aanspreekpunt Verwerker:

Manager Service Management / Information Security Officer
Bianca Brooijmans
eso@vanadgroup.com
010-288 16 00

Bij afwezigheid:


Manager Development & Innovation / Information Security Officer
Dré Lameir
eso@vanadgroup.com
010-288 16 00



## Informatiebeveiliging ZorgMail



Uitgave mei 2018

## Inhoud

1	ZorgMail oplossing.....	2
2	Gestructureerde berichten.....	2
3	Ongestructureerde berichten.....	3
3.1	Binnen de community.....	3
3.2	Tussen community's.....	3
3.3	Buiten de community.....	4
A.	Figuur 1: schematische weergave gestructureerde berichtenstromen.....	5
B.	Figuur 2: schematische weergave ongestructureerde berichtenstromen.....	6

## 1 ZorgMail oplossing

VANAD Enovation biedt met ZorgMail passende oplossingen voor grote en kleine (zorg)organisaties.

Om deelnemer te kunnen worden van ZorgMail vindt een screening van de aanmelding plaats door de Gebruikersadministratie van VANAD Enovation waarbij het verzoek onder meer wordt gecontroleerd op registratie in landelijke registers, zoals het AGB-code register, voordat tot acceptatie wordt overgegaan.

Gekoppelde organisaties en deelnemers zijn vindbaar in het ZorgMail adresboek. Als belangrijke schakel in de keten biedt VANAD Enovation als 'Trusted Third Party' veel toegevoegde waarde in het veilige berichtenverkeer tussen geauthentiseerde ZorgMail deelnemers evenals met deelnemers buiten de community.

Voor het veilig inloggen op ZorgMail applicaties wordt standaard gebruik gemaakt van Passage ID, een dienst van VANAD Enovation. Passage ID biedt de mogelijkheid aan gebruikers om het account te versterken met twee-staps-verificatie.

## 2 Gestructureerde berichten

ZorgMail EDI is een besloten dienst: de afzender en geadresseerde zijn bekend. Koppelingen van ZorgMail EDI met informatiesystemen vinden plaats op basis van door VANAD Enovation opgestelde technische beveiligingsspecificaties.

Authenticatie is mogelijk middels:

1. een X.509 client certificaat (/RSA Sleutelpaar)
2. een applicatiewachtwoord, Acces Key of API Key
3. een gebruikersnaam en wachtwoord is tevens mogelijk voor de informatiesystemen die nog geen client certificaat authenticatie voor EDI berichtenverkeer ondersteunen.

De berichten worden van afzender naar geadresseerde verstuurd over een onafhankelijk systeem (ZorgMail) van een onafhankelijke partij (VANAD Enovation) waarbij de verbindingen van en naar de centrale server end-to-end worden beveiligd. Voor systemen die dat ondersteunen bestaat de mogelijkheid om, naast de end-to-end versleuteling van de verbindingen, ook de berichten te versleutelen (S/MIME, PGP). Bij het gebruik van Internet als toegangsnetwerk wordt de verbinding tussen de software van de gebruiker en de server van ZorgMail versleuteld met TLS. Op de server van ZorgMail staat een server certificaat waarmee een versleutelde verbinding opgezet kan worden.

De gebruikersnaam en het wachtwoord voor authenticatie worden binnen de TLS-tunnel versleuteld verstuurd. De gebruiker heeft zelf geen certificaat nodig als de verbinding door de gebruiker wordt opgezet en voor authenticatie een gebruikersnaam en wachtwoord worden gebruikt. ZorgMail ondersteunt de nieuwste protocollen voor versleutelde verbindingen (TLS 1.2), aangevuld met een aantal gangbare protocollen waarvan geen ernstige kwetsbaarheden zijn gevonden. De protocolondersteuning wordt doorlopend beoordeeld en aangepast om het hoogste veiligheidsniveau te halen.

Zie ook figuur 1: “Schematische weergave gestructureerde berichtenstromen” in de bijlage.

## 3 Ongestructureerde berichten

Voor het veilig versturen van ongestructureerde berichten zoals e-mail zijn diverse mogelijkheden voorhanden. Zo is er de Veilig Verzenden button die zorgt dat het juiste afzenderadres wordt gehanteerd. Daarnaast wordt met deze button de geadresseerde voorafgaand aan de verzending gecontroleerd en de e-mail als vertrouwelijk gemarkeerd. Koppelingen van ZorgMail Secure e-mail met informatiesystemen vinden plaats op basis van door VANAD Enovation opgestelde technische/beveiligingsspecificaties.

Zie bijlag voor figuur 2: schematische weergave ongestructureerde berichtenstromen.

### 3.1 Binnen de community

ZorgMail Secure e-mail is de beveiligde oplossing van VANAD Enovation waarmee op veilige wijze tussen personen gecommuniceerd kan worden. Koppelingen met mailserveromgevingen worden op basis van door VANAD Enovation opgestelde technische/beveiligingsspecificaties gerealiseerd. De authenticatie van mailservers vindt plaats op basis van X.509 certificaten voor het benodigde vertrouwensniveau. In deze specificaties is ook beschreven hoe een deelnemer DKIM/SPF/DMARC maatregelen dient te nemen om mailvervalsing tegen te gaan. Voor de verbindingen wordt een sessie time-out bij inactiviteit gehanteerd van 20 minuten.

### 3.2 Tussen community's

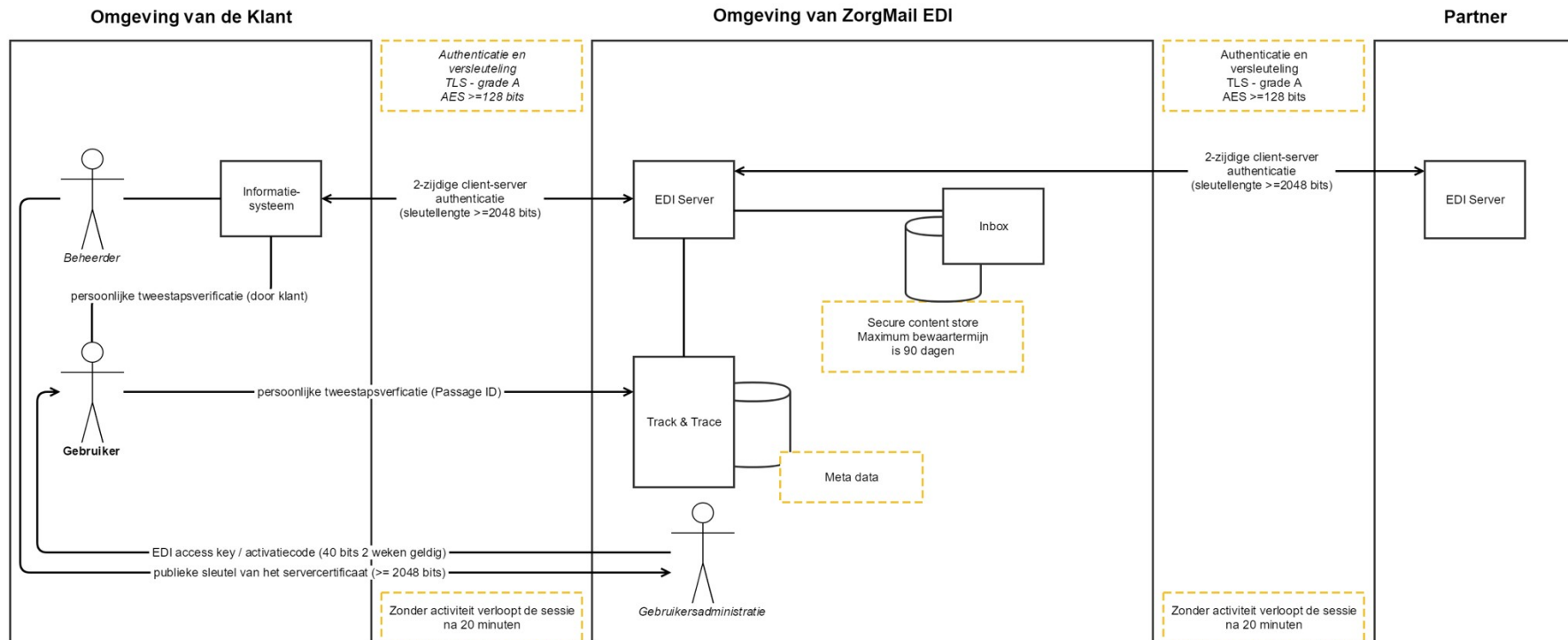
Ook kent ZorgMail koppelingen met netwerken van andere leveranciers die dienen te voldoen aan de beveiligingseisen die VANAD Enovation stelt. Met de leveranciers van deze gekoppelde netwerken zijn afspraken gemaakt hoe de adresboeken van toegelaten organisaties over en weer in de adresboeken up-to-date worden gehouden. De verbindingen zijn voorzien van de benodigde TLS encryptie (data in transit).



### 3.3 Buiten de community

Niet-ZorgMail deelnemers ontvangen een notificatiemail op hun internet e-mailadres. De niet-ZorgMail deelnemer krijgt via twee-staps-verificatie toegang tot het bericht gebruikmakend van de versleutelde ZorgMail omgeving. Koppelingen worden op basis van opgestelde technische/beveiligingsspecificaties gerealiseerd.

## A. Figuur 1: schematische weergave gestructureerde berichtenstromen



## B. Figuur 2: schematische weergave ongestructureerde berichtenstromen

