Reglement AVG- Privacybeleid **Gerritse & Hamelink Osteopathie** -Privacystatement

Op 25 mei 2018 zal de nieuwe Privacywetgeving in werking treden. Het gaat dan om Privacy Richtlijn (95/46/EG) en de Richtlijn privacy en elektronische communicatie (2002/58/EG), de nationale wetten ter uitvoering van deze richtlijnen en/of, in voorkomend geval, de verordening (EU) 2016/679 (de "Algemene Verordening Gegevensbescherming"). Een en ander samengevat als de AVG. Deze wetgeving zal de wet Bescherming persoonsgegevens vervangen. De AVG verwacht een meer pro-actieve rol van iedere organisatie die persoonsgegevens verwerkt. De meest relevante wijzigingen waar rekening mee dienen te worden gehouden zijn:

- versterking en uitbreiding van privacyrechten;
- meer verantwoordelijkheden voor organisaties;
- dezelfde, stevige bevoegdheden voor alle Europese privacytoezichthouders, zoals de bevoegdheid om boetes tot 20 miljoen euro op te leggen.

De Autoriteit Persoonsgegevens (hierna AP) blijft net als voorheen onder de wet Bescherming persoonsgegevens de autoriteit die controleert of organisaties zich aan de wetgeving houden. Ter voorbereiding op de nieuwe regelgeving heeft de AP een stappenplan opgesteld:

Het AVG-10 stappenplan:
1. Bewustwording
2. Rechten van betrokkenen
3. Overzicht verwerkingen
4. Data protection impact assessment (DPIA)
5. Privacy by design & privacy by default
6. Functionaris voor de gegevensbescherming
7. Meldplicht datalekken
8. Verwerkersovereenkomsten
9. Leidende toezichthouder
10. Toestemming

Een nadere uitwerking van dit stappenplan en naleving in de praktijk daarvan dient ervoor zorg te dragen dat **Gerritse & Hamelink Osteopathie** zich zoveel mogelijk aan de nieuwe wetgeving AVG kan houden. Hieronder zullen de verschillende stappen worden besproken. Daarbij wordt nagegaan in hoeverre deze punten binnen **Gerritse & Hamelink Osteopathie** gelden, waar **Gerritse & Hamelink Osteopathie** tegen aan loopt en op welke wijze **Gerritse & Hamelink Osteopathie** op een verantwoorde manier aan de 'nieuwe' verplichtingen kan voldoen.

1 Bewustwording

1. **Gerritse & Hamelink Osteopathie** is een groepspraktijk waarbinnen meerdere osteopaten osteopathie als dienstverlening aanbiedt. Om dat doel te kunnen uitvoeren dient **Gerritse & Hamelink Osteopathie** persoonsgegevens van patiënten te verwerken en gebruiken binnen de dagelijkse bedrijfsvoering.

2. De gegevens die worden gedocumenteerd zijn privacy gevoelig. Het gaat om persoonsgegevens, aan de hand waarvan de betrokkene zowel direct als indirect geïdentificeerd kan worden. Ten einde er zeker van te zijn dat met die gegevens wordt omgegaan op een wijze die verantwoord is en voldoet aan de privacy wetgeving zoals per 25 mei 2018 van kracht zal worden heeft **Gerritse & Hamelink Osteopathie** ervoor gekozen met

het onderhavige protocol in kaart te brengen, aan de hand van het AVG stappenplan (zoals hiervoor opgesomd), op welke wijze invulling gegeven dient te worden aan de AVG.

3. Het betreft hier registratie van persoonsgegevens met een gerechtvaardigd belang. Immers de patiënten melden zich zelf aan bij **Gerritse & Hamelink Osteopathie.** Zij willen graag geholpen worden door de osteopaat voor hun klachten.

2. Rechten van betrokkenen

2.1 Om een eerlijke verwerking van persoonsgegevens te waarborgen geeft de Verordening diverse rechten aan de betrokkene. De betrokkene kan deze rechten uitoefenen tegen de verwerkingsverantwoordelijke. De betrokkene heeft:
- het recht op informatie over de verwerkingen;
- het recht op inzage in zijn gegevens;
- het recht op correctie van de gegevens als deze niet kloppen;
- het recht op verwijdering van de gegevens en 'het recht om vergeten te worden';
- het recht op beperking van de gegevensverwerking;
- het recht op verzet tegen de gegevensverwerking;
- het recht op overdracht van zijn gegevens (dataportabiliteit);
- het recht om niet onderworpen te worden aan een geautomatiseerde besluitvorming.

2.2 Een patiënt of voormalig patiënt (de betrokkene) kan om bovenstaande gegevens verzoeken. De betrokkene kan zulks doen per mail naar info@gh-osteopathie.nl. De betrokkene dient zich daarbij te legitimeren, opdat **Gerritse & Hamelink Osteopathie** met voldoende zekerheid kan vaststellen dat degene die het verzoek doet daadwerkelijk de betrokkene is.

2.3 **Gerritse & Hamelink Osteopathie** zal binnen 1 maand na ontvangst van het verzoek betrokken informeren over de uitvoering van het verzoek. Bij complexe, of een veelvoud aan verzoeken kan deze termijn verlengd worden met maximaal 2 maanden. De betrokkene zal in een dergelijk geval van verlengde termijn van uitvoering van het verzoek daaromtrent geïnformeerd worden. De informatie wordt in principe schriftelijk verstrekt.

2.4 In sommige gevallen mag **Gerritse & Hamelink Osteopathie** weigeren tot uitvoering van het verzoek om gegevensverstrekking over te gaan, dan wel daarvoor kosten in rekening brengen. Het moet dan gaan om de situatie dat de betrokkene buitensporige of ongegronde verzoeken doet. (Bijvoorbeeld meerdere verzoeken achter elkaar om dezelfde gegevens. Dan wel wanneer sprake is van een van de beschermende noodzakelijkheidscriteria welke de AVG kent zoals bijvoorbeeld in het kader van een (strafrechtelijk) onderzoek naar de betrokkene). Indien **Gerritse & Hamelink Osteopathie** weigert aan het verzoek te voldoen, zal **Gerritse & Hamelink Osteopathie** zulks motiveren en de betrokkene wijzen op het klachtrecht bij de toezichthouder AVG.

2.5 **Gerritse & Hamelink Osteopathie** realiseert zich dat indien zij een schriftelijke beslissing neemt in het kader van de uitoefening van de rechten van de betrokkene, dat dit dan geldt als een besluit in de zin van de Algemene wet bestuursrecht.

2.6 In sommige gevallen dient **Gerritse & Hamelink Osteopathie** de betrokken patiënt uit zichzelf te informeren. Dit is het geval indien:
- gegevens buiten de betrokkene om worden verkregen

- gegevens voor een ander doel gebruikt gaan worden dan waar de gegevens oorspronkelijk voor waren afgegeven. **Gerritse & Hamelink Osteopathie** zal in die gevallen binnen 1 maand betrokkene informeren.

2.7 Indien de behandeling van de patiënt eindigt zal **Gerritse & Hamelink Osteopathie** de persoonsgegevens nog enige tijd in haar systeem bewaren. De wet Wgbo bepaalt dat medische dossiers 15 jaar moeten worden bewaard. Aan die bewaartermijn zal **Gerritse & Hamelink Osteopathie** zich houden. De dossiers zullen na 15 jaar vernietigd worden. Binnen het dossier bevinden zich tevens gegevens van niet medische aard.

2.8 Ten einde er zeker van te zijn dat de betrokkene een volledig beeld heeft van de wijze waarop met diens persoonsgegevens wordt omgegaan en met welk doel en onder welke grondslag (gerechtvaardigd belang), zal iedere betrokken bij registratie toegang krijgen tot deze privacystatement en de hierbij behorende documenten. **Gerritse & Hamelink Osteopathie** zal deze gegevens op de website plaatsen en iedere betrokkene op die vindplaats wijzen.

3. Register van verwerkingsactiviteiten

1.1. **Gerritse & Hamelink Osteopathie** verwerkt persoonsgegevens van patiënten. De volgende persoonsgegevens worden van deze leden verwerkt. Ten aanzien van al deze vormen van verwerkingen van persoonsgegevens zal **Gerritse & Hamelink Osteopathie** een register van verwerkingsactiviteiten bijhouden. Daarin worden alle soorten persoonsgegevens die verwerkt zullen worden opgenoemd.

2. In het geval de patiënt een klacht indient tegen de osteopaat, zullen die gegevens eveneens worden verwerkt door **Gerritse & Hamelink Osteopathie**.

4 DPIA (Data protection impact assessment)

4.1 DPIA staat voor gegevensbeschermingseffectbeoordeling. Een DPIA is alleen verplicht wanneer sprake is van gegevensverwerking welke waarschijnlijk een hoog privacyrisico oplevert. Binnen de AVG worden drie situaties besproken wanneer sprake is van verhoogd risico.:

- systematisch en uitvoerig persoonlijke aspecten evalueren
- op grote schaal bijzondere persoonsgegevens verwerken
- op grote schaal en systematisch mensen volgen in een publiek toegankelijk gebied

4.2 Naast de criteria uit de AVG zelf heeft de werkgroep van Europese privacytoezichthouders een lijst met 9 criteria opgesteld om nader te bezien of een DPIA nodig is. De criteria die op osteopaten van toepassing zouden kunnen zijn:

- gevoelige gegevens verwerking
- grootschalige gegevens verwerking
- gegevensverwerking over kwetsbare personen

4.3 De privacytoezichthouders zien verwerkingen van bijzondere persoonsgegevens door individuele artsen niet als grootschalig. Individuele artsen hoeven dus geen DPIA uit te voeren. Het ligt voor de hand dat de gegevensverwerking door de individuele osteopaat

aldus evenmin de uitvoering van een DPIA behoeft. **Gerritse & Hamelink Osteopathie** zal zodoende geen DPIA uitvoeren.

4.4 Evenwel is **Gerritse & Hamelink Osteopathie** zich ervan bewust dat sprake is van bijzondere persoonsgegevens. De inhoud van een medisch dossier is gevoelig voor de betrokkene en vergt een grote mate van vertrouwelijkheid. **Gerritse & Hamelink Osteopathie** zal zich zodoende inzetten die gegevens vertrouwelijk te laten blijven.

4.5 De gegevens zoals **Gerritse & Hamelink Osteopathie** registreert zijn slechts bedoeld voor intern gebruik. De persoonsgegevens worden gebruikt om te waarborgen dat de osteopaat de patiënt zo goed mogelijk van dienst kan zijn. Van dienst zijn in het verhelpen van de klachten en van dienst zijn door het mogelijk maken dat de ziektekostenverzekering de kosten zoveel mogelijk vergoedt.

4.6 Op termijn zal de Autoriteit Persoonsgegevens (AP) een lijst van verwerkingen publiceren waar een DPIA voor verplicht is. Zodra die lijst er is, zal osteopathie Gerritse haar verwerking van persoonsgegevens opnieuw tegen het licht houden om te bezien of nog nadere maatregelen nodig zijn.

5. Privacy by design & privacy by default

5.1. Privacy door ontwerp en door standaardinstellingen voor producenten. **Gerritse & Hamelink Osteopathie** is producent van een dienst, welke wordt ondersteund door de verwerking van persoonsgegevens. Zodoende houdt **Gerritse & Hamelink Osteopathie** bij de ontwikkeling en uitwerking van die dienst rekening met het recht op bescherming van persoonsgegevens. Met inachtneming van de stand van de techniek ziet **Gerritse & Hamelink Osteopathie** erop toe dat de verwerkingsverantwoordelijken en de verwerkers in staat zijn te voldoen aan hun verplichtingen inzake gegevensbescherming.

5.2. **Gerritse & Hamelink Osteopathie** let daarbij op:

- het minimaliseren van de verwerking van persoonsgegevens;
- slechts het BSN nummer noteren, doch geen kopie maken van de het paspoort/ID kaart;
- transparantie met betrekking tot de functies en de verwerking van persoonsgegevens;
- het in staat stellen van de betrokkene om controle uit te oefenen op de informatieverwerking; en
- beveiligingskenmerken creëren en verbeteren.

6. Functionaris voor de gegevens bescherming

6.1. Net als voor de DPIA geldt dat de individuele praktijk van een osteopaat door de AP niet wordt gezien als een grootschalige verwerker. Het instellen van een FG is ondanks dat het gaat om bijzondere persoonsgegevens niet noodzakelijk. Daarbij stipt **Gerritse & Hamelink Osteopathie** nogmaals aan dat in deze sprake is van het verwerken van persoonsgegevens op verzoek van de patiënt, nu deze een zo goed mogelijke behandeling wenst. **Gerritse & Hamelink Osteopathie** verwerkt geen persoonsgegevens voor commerciële doeleinden.

Patiënten worden niet gevolgd door **Gerritse & Hamelink Osteopathie** aan de hand van de persoonsgegevens.

6.2. **Gerritse & Hamelink Osteopathie** benadrukt opnieuw zich te realiseren persoonsgegevens te verwerken die een hoge mate van vertrouwelijkheid kennen. **Gerritse & Hamelink Osteopathie** meent echter alle maatregelen te hebben genomen, ten einde erop toe te zien dat de persoonsgegevens van patiënten niet voor andere doeleinden gebruikt worden dan bedoeld is.

7. Meldplicht Datalekken

7.1. Een datalek in de zin van de AVG is een inbreuk in verband met persoonsgegevens. Het is een inbreuk op de beveiliging die leidt tot de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens.

7.2. Het is voor de kwalificatie als 'inbreuk in verband met persoonsgegevens' niet relevant dat er boze opzet in het spel is. Naast het 'hacken' van persoonsgegevens, kan ook gedacht worden aan gegevens die op een verloren laptop staan of een afgesloten website met persoonsgegevens die per ongeluk openstaat. Een inbreuk op de beveiliging houdt in dat zich daadwerkelijk een beveiligingsincident heeft voorgedaan. Er is niet uitsluitend sprake van een dreiging, of van een tekortkoming in de beveiliging (ook wel aangeduid als een beveiligingslek) die zou kunnen leiden tot een beveiligingsincident. Er heeft zich daadwerkelijk een beveiligingsincident voorgedaan, waarbij de getroffen preventieve maatregelen niet toereikend waren om dit te voorkomen.

7.3. **Gerritse & Hamelink Osteopathie** zal ieder datalek aan de AP melden, tenzij onwaarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. **Gerritse & Hamelink Osteopathie** zal binnen 72 uur na ontdekking de AP in kennis stellen, ook indien nog niet alle informatie voorhanden is.

7.4. Bovendien zal **Gerritse & Hamelink Osteopathie** het datalek onverwijld melden aan de betrokkenen, indien sprake is van een hoog risico door de inbreuk op de persoonsgegevens. Voor de vraag of sprake is van een hoog risico zal **Gerritse & Hamelink Osteopathie** eerst nader onderzoek daar naar mogen doen.

7.5. Het datalek zal door **Gerritse & Hamelink Osteopathie** gedocumenteerd worden in een overzicht van datalekken die zich binnen **Gerritse & Hamelink Osteopathie** hebben voorgedaan. Niet alleen zullen de feiten omtrent de inbreuk en de gevolgen daarvan in dit overzicht worden gedocumenteerd, doch eveneens de genomen corrigerende maatregelen.

8. Verwerkersovereenkomsten

8.1. **Gerritse & Hamelink Osteopathie** maakt gebruik van Crossuite voor het verwerken van de persoonsgegevens in een patiëntenbeheerplatform. Dit bedrijf dient zodoende gezien te worden als een verwerker. Ten einde ervan verzekerd te zijn dat crossuite zich aan de vereisten houdt welke nodig zijn om te voldoen aan de AVG heeft **Gerritse & Hamelink Osteopathie** een verwerkersovereenkomst afgesloten met Crossuite.

8.2. Binnen de verwerkersovereenkomst met Crossuite zijn in ieder geval de volgende zaken geregeld:

- het onderwerp en de duur van de verwerking;
- de aard en het doel van de verwerking;
- het soort persoonsgegevens en de categorieën van betrokkenen;
- de rechten en verplichtingen van de verwerkingsverantwoordelijke.
- de persoonsgegevens alleen verwerkt worden onder schriftelijke instructie van **Gerritse & Hamelink Osteopathie**, onder andere voor wat betreft de doorgifte van persoonsgegevens aan een derde land of een internationale organisatie (tenzij deze daartoe wettelijk is verplicht);
- waarborg van de verwerker dat de toegang tot die gegevens is beperkt tot gemachtigde personen. Deze personen moeten gebonden zijn aan geheimhouding op grond van een overeenkomst of een wettelijke verplichting;
- de verwerker minimaal hetzelfde niveau van beveiliging van de persoonsgegevens hanteert als **Gerritse & Hamelink Osteopathie** doet;
- de verwerker zal **Gerritse & Hamelink Osteopathie** alle mogelijke ondersteuning bieden bij het nakomen van haar verplichtingen met het oog op beantwoording van verzoeken rondom de rechten van betrokkenen;
- verwerker **Gerritse & Hamelink Osteopathie** zal bijstaan bij het nakomen van haar verplichtingen op het gebied van beveiliging van persoonsgegevens en de meldplicht datalekken;
- na beëindiging van de overeenkomst tussen **Gerritse & Hamelink Osteopathie** en verwerker, de in uw opdracht verwerkte persoonsgegevens wist of aan **Gerritse & Hamelink Osteopathie** teruggeeft, en bestaande kopieën verwijdert;
- **Gerritse & Hamelink Osteopathie** alle informatie ter beschikking stelt die nodig is om aantoonbaar te maken dat de verplichtingen op grond van de Verordening rondom het inzetten van een verwerker worden nageleefd en die nodig is om audits mogelijk te maken;
- verwerker maakt inzichtelijk welke afspraken deze met betrekking tot sub-verwerkers maakt;
- verwerker vermeldt de goedgekeurde gedragscodes en certificeringsmechanismen waar verwerker bij diens werkzaamheden gebruik van maakt;
- verwerker garandeert **Gerritse & Hamelink Osteopathie** aan alle verplichtingen te voldoen zoals de AVG van verwerker verlangt.

8.3 **Gerritse & Hamelink Osteopathie** maakt geen gebruik van andere verwerkers dan Crossuite. Wel maakt **Gerritse & Hamelink Osteopathie** gebruik van een boekhouder. Deze verwerkt geen gegevens van patiënten, maar heeft wel inzage in sommige persoonsgegevens. Vooral de gegevens rondom betalingen zal de boekhouder in kunnen zien. Zodoende heeft boekhouder een geheimhoudingsverklaring ondertekend. In die verklaring wordt niet alleen weergegeven dat de boekhouder zelf geheimhouding zal betrachten over alle persoonsgegevens die deze te zien krijgt van patiënten van **Gerritse & Hamelink Osteopathie,** ook de medewerkers en derden waar de boekhouder gebruik van maakt hebben diezelfde geheimhoudingsplicht. Bovendien is in de verklaring opgenomen dat de boekhouder geen persoonsgegevens van patiënten zal verwerken.

9. Leidende Toezichthouder

9.1. **Gerritse & Hamelink Osteopathie** dient te bepalen onder welke toezichthouder zij valt. **Gerritse & Hamelink Osteopathie** heeft 3 vestiging te Westdorpe., Hulst en Terneuzen. Dit is op Nederlandse bodem. De werkzaamheden van **Gerritse & Hamelink Osteopathie** rusten op

Nederlands grondgebied. De Leidende toezichthouder voor **Gerritse & Hamelink Osteopathie** is dus de Autoriteit Persoonsgegevens te Nederland.

10. Toestemming

10.1. Voor de verwerking van bepaalde gegevens is toestemming nodig van de betrokkene. Dat is het geval indien het gaat om bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard. Ook het nationaal identificatienummer (BSN) is een zaak waarbij expliciete toestemming van de betrokkene nodig is, indien dat nummer wordt verwerkt. **Gerritse & Hamelink Osteopathie** verwerkt het BSN nummer van haar patiënten nu Osteopaten verplicht zijn dit nummer te gebruiken in correspondentie met andere zorgverleners. Het verwerken van gegevens over de gezondheid betreft eveneens een bijzondere categorie gegevens waarvan voor de verwerking toestemming nodig is van de patiënt. Het heeft echter de sterke voorkeur het verwerken van alle persoonsgegevens op voorhand met patiënten te bespreken en bij die verwerking expliciet te vermelden of de patiënt toestemming heeft gegeven voor die verwerking.

10.2. **Gerritse & Hamelink Osteopathie** zal op de volgende wijze invulling geven aan deze benodigde toestemming. Naast het opstellen van een behandelplan zal bij de intake van een patiënt een overzicht worden gegeven van de afspraken. Deze zullen met de patiënt worden doorgenomen en vervolgens aan de patiënt ter hand worden gesteld dan wel aan de patiënt worden verzonden per mail, waarbij aangetekend wordt dat het hier een bevestiging van de gemaakte afspraken betreft. Er zal om een ontvangstbevestiging worden verzocht bij de patiënt. Op deze 'opdrachtbevestiging' zullen de belangrijkste gegevens worden benoemd over wat de patiënt kan verwachten van de osteopaat. Het gaat om het volgende:

- dat patiënt is gewezen op het feit dat persoonsgegevens verwerkt zullen worden en om welke persoonsgegevens het gaat;
- dat patiënt voor die verwerking expliciet toestemming heeft verleend;
- dat patiënt rechten heeft ten aanzien van het verwerken van persoonsgegevens en dat patiënt deze en de verdere werkwijze van **Gerritse & Hamelink Osteopathie** met betrekking tot die persoonsgegevens kan nalezen in het onderhavige reglement zoals op de website van **Gerritse & Hamelink Osteopathie** staat vermeld;
- dat patiënt gewezen wordt op de bewaartermijn(en) van de persoonsgegevens;
- dat patiënt de mogelijkheid heeft een klacht tegen **Gerritse & Hamelink Osteopathie** in te dienen bij het NRO of NOF;
- wat het consulttarief is van **Gerritse & Hamelink Osteopathie**

11. Slotwoord

11.1 **Gerritse & Hamelink Osteopathie** gaat ervan uit met dit privacybeleid aan alle vereisten van de nieuwe AVG regels te voldoen. **Gerritse & Hamelink Osteopathie** is zich ervan bewust dat sprake is van nieuwe regelgeving en dat zulks inhoudt dat nog niet alle facetten zich even makkelijk laten uiteenzetten. **Gerritse & Hamelink Osteopathie** zal de aanpassingen, beslissingen en verder nieuws vanuit de AP volgen, opdat tijdige maatregelen genomen kunnen worden deze beleidsregels alsnog verder aan te scherpen, of bij te snijden.

Register van Verwerkingsactiviteiten van:

Gerritse & Hamelink Osteopathie

Herengracht 15

4531 GM Terneuzen

- **Doel**
    - Op 25 mei 2018 zal de nieuwe Privacywetgeving in werking treden. Onderdeel daarvan is de verordening (EU) 2016/679, de Algemene Verordening Gegevensbescherming (AVG). Deze verordening schrijft voor dat iedere organisatie waarin persoonsgegevens worden verwerkt een register van verwerkingen opstelt. Met onderhavige register wordt aan die verplichting voldaan
    - Een osteopaat verwerkt persoonsgegevens van diens patiënten. Naast identificatiegegevens van de patiënt wordt een medisch dossier aangelegd. Het betreft aldus privacy gevoelige informatie.

- **Beveiliging**
    - Om er zeker van te zijn dat deze gegevens zo veilig mogelijk verwerkt worden is gebruik gemaakt van de volgende beveiliging.

1. Naam ICT bedrijf: Crossuite. Contactpersoon: Steve de Jongh
2. Voor de waarborging van uw privacy verwijs ik naar de verwerkerovereenkomst die afgesloten is met de firma crossuite, deze is te downloaden op onze website: info@gh-osteopathie.nl
3. De online dienst crossuite wordt geopend vanuit mijn laptop die beveiligd is met een paswoord. Als crossuite wordt geopend wordt ook gevraagd naar een inlog en een paswoord dat alleen te verkrijgen is via een gridcard. Tevens is er beveiliging via het mailadres van ons waar een code naartoe gestuurd wordt.

2.2. Buiten de genoemde systemen zal geen ander systeem gebruikt worden om gegevens te verwerken. Patiëntengegevens zullen niet op andere datatransmitters zoals laptops, usbsticks, harde schijf, geplaatst worden.

- **Ontvangers van data**

3.1. Patiëntengegevens zullen enkel na afgegeven machtiging door de patiënt worden verstrekt aan derden. Het betreft dan derden waarvan de patiënt schriftelijk toestemming heeft gegeven om met de patiënt afgestemde gegevens aan te verstrekken. Dit kunnen artsen, andere zorgverleners, advocaten of andere juridische dienstverleners zijn.

3.2. In het dossier van de patiënt zal nauwkeurig worden bijgehouden welke gegevens op verzoek van de patiënt met derden zijn gedeeld.

3.3. Indien gegevens internationaal worden gedeeld, zal dit in principe door de patiënt zelf worden gedaan, nu daarvoor extra waarborgen gelden.

- **Categorieën van persoonsgegevens en bewaartermijnen**

4.1. Alle medische gegevens en gegevens welke nodig zijn om de medische gegevens goed te bewaren kennen een wettelijke bewaartermijn van 15 jaren op grond van de wet op de geneeskundige behandelingsovereenkomst (Wgbo).

Voornaam, achternaam	BSN
Geboortedatum	Huisarts
Straat, huisnummer, postcode, plaats, land	Verzekering, polisnummer
Emailadres, telefoonnummer	Gewicht en lengte
Medische historie, zoals voorgeschreven medicatie	Beroep, hobby's, sport
Ondergane operaties, ziekten, familiare aandoeningen	Wijze waarop patiënt bij osteopaat is terechtgekomen
Ongevallen/gebeurtenissen, verrichte onderzoeken	Welke taal spreekt patiënt
Specificaties op gebied van hart en vaatziekten, longen, spijsvertering, urogenitaal en hormonaal vlak	Eventuele klacht die patiënt tegen osteopaat heeft ingediend
Anamnese: klacht omschrijving sinds wanneer ervaart men klacht, provocerende factoren, reducerende factoren, bijkomende klachten, eerdere behandelingen	Onderzoek: Biomechanisch, respiratoir/ circulatoir, bio-energetisch/ metabool, Neurologisch, Biopsychosociaal
Consultatie patiënt; journaal en behandelingen	Osteopatische diagnose; osteopathische conclusie, verwachting mbt herstel, indicatie voor osteopathie
Documenten indien van toepassing: verslag verwijzer, verslag naar doorverwijzing, verslag aan derden op verzoek patiënt, verslag laboratorium onderzoek/röntgenonderzoek, ander onderzoek	

Verwerkersovereenkomst

TUSSEN:

1. Gerritse & Hamelink Osteopathie, statutair gevestigd en kantoorhoudend aan de `Herengracht 15 4531GM Terneuzen, ingeschreven bij de Kamer van Koophandel onder nummer , hierna te noemen '**Verantwoordelijke'**; en

2. Firma Crossuite, hierna te noemen '**Verwerker'**,

Samen de '**Partijen**'.

ACHTERGROND:

a. Op [datum], hebben Partijen een overeenkomst gesloten (de '**Hoofdovereenkomst**') met kenmerk en/of referentienummer [kenmerk vermelden] op grond waarvan Verwerker persoonsgegevens van Verantwoordelijke verwerkt;

b. Privacywetgeving, inclusief nationale wetten ter uitvoering van de Privacyrichtlijn en de Algemene Verordening Gegevensbescherming, vereist dat dergelijke verwerkingen worden geregeld door een overeenkomst of rechtshandeling die de Verwerker bindt aan de Verantwoordelijke en waarin het onderwerp en de duur van de verwerking, de aard en het doel van de verwerking, de verplichtingen van de Verwerker in verband met beveiligingsincidenten en datalekken, het soort persoonsgegevens en de categorieën van betrokkenen, en de rechten en verplichtingen van de Verantwoordelijke worden omschreven; en

c. Partijen wensen de bovenstaande vereisten in de onderhavige verwerkersovereenkomst (de '**Verwerkersovereenkomst**') te regelen, welke overeenkomst een integraal onderdeel is van de Hoofdovereenkomst.

Partijen verklaren te zijn overeengekomen als volgt:

1. Definities en Interpretatie

1.1. '**Betrokkene'**, '**Persoonsgegevens'**, '**Verantwoordelijke'**, en '**Verwerker'** hebben de betekenis zoals bedoeld in de Privacywetgeving. Daarnaast hebben de volgende woorden en zinsdelen de volgende betekenis:

'**Beveiligingsincident**' een daadwerkelijke, verwachte of vermoede i) schending van technische en organisatorische beveiligingsmaatregelen welke leidt tot onbedoelde of onrechtmatige vernietiging, verlies, wijziging, onbevoegde openbaarmaking of toegang tot gegevens, met inbegrip van Persoonsgegevens, ii) schending van Privacywetgeving of deze Verwerkersovereenkomst door een huidige of voormalige werknemer, aannemer of agent van de Verwerker of door een andere persoon of derde, en/of iii) gebeurtenis waarbij de beveiliging, vertrouwelijkheid, integriteit of

	beschikbaarheid van gegevens, waaronder Persoonsgegevens, zijn of redelijkerwijs kunnen zijn gecompromitteerd;
'**Privacywetgeving**'	de Privacy Richtlijn (95/46/EG) en de Richtlijn privacy en elektronische communicatie (2002/58/EG), de nationale wetten ter uitvoering van deze richtlijnen en/of, in voorkomend geval, de verordening (EU) 2016/679 (de "**Algemene Verordening Gegevensbescherming**") en elke wetgeving of verordening die het voorgaande van tijd tot tijd wijzigt of aanvult;

1.2. In geval van inconsistentie tussen de bepalingen van deze Verwerkersovereenkomst en de Hoofdovereenkomst, gelden de bepalingen van deze Verwerkersovereenkomst.

1.3. In geval van nietigheid c.q. vernietigbaarheid van een of meer bepalingen uit deze Verwerkersovereenkomst blijven de overige bepalingen onverkort van kracht.

2. Werkzaamheden Verwerker

2.1. De voorwaarden van deze Verwerkersovereenkomst zijn van toepassing op de Persoonsgegevens die de Verwerker, of de toegestane onderaannemers, verwerken tijdens het verlenen van diensten in het kader van de Hoofdovereenkomst, zoals weergegeven in Annex 1. Partijen komen overeen dat de Verantwoordelijke de verwerkingsverantwoordelijke van de Persoonsgegevens is of een verwerker van Persoonsgegevens namens een andere verwerkingsverantwoordelijke. Partijen komen verder overeen dat Verwerker de Persoonsgegevens verwerkt in het kader van uitvoering van de Hoofdovereenkomst.

2.2. De Verwerker verwerkt alleen die Persoonsgegevens zoals verder gespecificeerd in Annex 1 en voert deze verwerkingshandelingen alleen uit met betrekking tot de uit de Hoofdovereenkomst voortvloeiende en in deze Verwerkersovereenkomst of anderszins goedgekeurde met voorafgaande schriftelijke toestemming van de Verantwoordelijke nader beschreven aard en doeleinden van de verwerking, onder voorbehoud van Artikel 2.4 van deze Verwerkersovereenkomst. Verwerker zal in dit kader alle redelijke instructies van de Verantwoordelijke in verband met de verwerking opvolgen.

2.3. De Verwerker verwerkt geen Persoonsgegevens voor zijn eigen doeleinden of die van anderen, tenzij i) een op de Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling hem tot verwerking verplicht; in dat geval stelt de Verwerker de Verantwoordelijke, voorafgaand aan de verwerking, in kennis van dat wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt of ii) Verantwoordelijke daartoe nadere schriftelijke instructies heeft gegeven.

2.4. De Verwerker verwerkt de Persoonsgegevens in overeenstemming met de Privacywetgeving die van toepassing is op de verwerking van Persoonsgegevens onder deze Verwerkersovereenkomst, waarbij ook rekening wordt gehouden met afzonderlijke verplichtingen die de Verantwoordelijke krachtens Privacywetgeving kan hebben. De Verwerker stelt de Verantwoordelijke onmiddellijk in kennis wanneer een instructie van de Verantwoordelijke betreffende de verwerking van Persoonsgegevens naar haar mening inbreuk maakt op Privacywetgeving of andere toepasselijke wetgeving.

2.5. De Verwerker zorgt ervoor dat alle Persoonsgegevens die door de Verwerker zijn gecreëerd namens de Verantwoordelijke nauwkeurig zijn en zo nodig bijgewerkt worden en zorgt ervoor dat de Persoonsgegevens die onjuist of onvolledig zijn worden gewist of gerectificeerd overeenkomstig de instructies van de Verantwoordelijke.

2.6. In aanvulling op het voorgaande lid 5 van dit Artikel leggen Partijen vast dat Verwerker de Persoonsgegevens aantoonbaar, op behoorlijke en zorgvuldige wijze zal verwerken en in overeenstemming met de op hem als Verwerker rustende verplichtingen op grond van de

Privacywetgeving of andere toepasselijke wetgeving. Verwerker zal in dat kader ten minste een register van verwerkingen aanleggen als bedoeld in Artikel 30 AVG en op eerste verzoek van Verantwoordelijke zal Verwerker een kopie van dat register verstrekken.

2.7. De Verwerker zal geen Persoonsgegevens verwerken in- of doorgeven aan een land, gebied of organisatie buiten de Europese Economische Ruimte ("EER") zonder voorafgaande schriftelijke toestemming van de Verantwoordelijke (en de Verwerker zorgt ervoor dat elke onderaannemer aan hetzelfde voldoet).

3. Beveiliging

3.1. De Verwerker ontwikkelt, implementeert en onderhoudt een uitgebreid schriftelijk informatiebeveiligingsbeleid dat vereist dat de Verwerker passende technische en organisatorische maatregelen neemt om Persoonsgegevens, in het licht van de huidige stand van de techniek, te beschermen tegen inbreuken op beveiliging, vertrouwelijkheid of integriteit en andere ongeautoriseerde of onwettige vormen van verwerking. Zulke maatregelen zullen een passend veiligheidsniveau garanderen, rekening houdend met de risico's die bij de verwerking betrokken zijn, met name door ongevallen of onwettige vernietiging, verlies, wijziging, onbevoegde openbaarmaking of toegang tot persoonsgegevens die worden overgedragen, opgeslagen of anderszins verwerkt, gebaseerd op de aard van de persoonsgegevens, geldende industrie standaarden en verplichte veiligheidseisen die van toepassing zijn op de verwerker.

3.2. Naast de algemene verplichting uit hoofde van Artikel 3.1, omvatten dergelijke technische en organisatorische beveiligingsmaatregelen ten minste de beveiligingsmaatregelen in Annex 2 van deze Verwerkersovereenkomst.

3.3. De Verwerker zorgt ervoor dat het personeel dat bevoegd is om de Persoonsgegevens te verwerken zich tot vertrouwelijkheid verbindt gedurende en na hun dienstverband (bijvoorbeeld door middel van een geheimhoudingsovereenkomst), voor zover het niet reeds tot een wettelijke verplichting tot geheimhouding is gehouden.

3.4. De partijen erkennen dat de in dit Artikel 3 bedoelde technische en organisatorische maatregelen in de loop van de tijd kunnen veranderen en dat effectieve beveiligingsmaatregelen regelmatige evaluatie en verbetering van de maatregelen vereisen. De Verwerker zal deze maatregelen derhalve regelmatig evalueren, aanscherpen en/of verbeteren om te (blijven) voldoen aan de eisen en verplichtingen zoals genoemd in dit Artikel 3.

4. **Beveiligingsincidenten**

4.1. De Verwerker zorgt voor adequate beveiligingsmaatregelen en neemt de technische en organisatorische beveiligingsmaatregelen die nodig zijn in verband met de toepasselijke wettelijke verplichtingen die van toepassing zijn op de Verwerker en de Verantwoordelijke inzake Beveiligingsincidenten.

4.2. In geval van een Beveiligingsincident zal de Verwerker de Verantwoordelijke onverwijld op de hoogte stellen via een kennisgeving, maar uiterlijk 12 uur nadat de Verwerker of een onderaannemer zich bewust is van een dergelijk Beveiligingsincident en op een zodanige wijze dat de Verantwoordelijke kan voldoen aan van toepassing zijnde wetgeving betreffende Beveiligingsincidenten, met name relevante kennisgevingsvereisten in verband met Beveiligingsincidenten en inbreuken op de beveiliging van Persoonsgegevens. Een kennisgeving van een Beveiligingsincident mag in beginsel mondeling geschieden, maar dient altijd gevolgd te worden door een schriftelijke bevestiging aan Verantwoordelijke.

4.3. Niet tegenstaande de verplichtingen van de Verwerker onder Artikel 4.2, bevat de kennisgeving van de Verwerker tenminste de punten in Annex 3, waarbij de Verwerker zich rekenschap geeft van het belang van een onverwijlde melding, alsook de mogelijkheid om eerdere kennisgevingen op te volgen en aan te vullen.

4.4. Zodra de Verwerker op de hoogte is van een Beveiligingsincident, moet de Verwerker alle noodzakelijke en passende maatregelen nemen om de gevolgen van het Beveiligingsincident te onderzoeken, te reduceren en te herstellen en de Verantwoordelijke te helpen ervoor te zorgen dat de Verantwoordelijke kan voldoen aan de Privacywetgeving en eventuele wettelijke en/of contractuele verplichtingen (zoals verplichtingen om derden in kennis te stellen, inclusief toezichthouders en betrokkenen) in verband met het Beveiligingsincident. Dit betekent, met zoveel woorden, dat de Verwerker te allen tijde zijn medewerking verleent aan Verantwoordelijke in het kader van het hiervoor gestelde en eventuele nadere instructies van de Verantwoordelijke adequaat zal opvolgen.

4.5. Verwerker dient zich te onthouden van het op enigerlei wijze verstrekken van of delen van informatie over Beveiligingsincidenten aan derde partijen en/of betrokkenen, behoudens voor zover Verwerker daartoe wettelijk verplicht is of Partijen anderszins zijn overeengekomen.

5. Samenwerking en betrokkenen

5.1. De Verwerker zal de Verantwoordelijke binnen 24 uur in kennis stellen, tenzij uitdrukkelijk door toepasselijke wetgeving verboden, in geval van i) een klacht in verband met de verwerking van Persoonsgegevens onder de Verwerkersovereenkomst, ii) een verzoek, vraag of bevel tot de productie, verwerking of toegang tot persoonsgegevens, of iii) verzoeken van betrokkenen, waaronder verzoeken tot toegang, rectificatie, blokkering van verwerking van persoonsgegevens, data-overdraagbaarheid en soortgelijke verzoeken. De Verwerker reageert niet op dergelijke verzoeken, tenzij met voorafgaande toestemming van de Verantwoordelijke; De Verwerker werkt op dit punt samen met de Verantwoordelijke en ondersteunt de Verantwoordelijke bij het afhandelen en beantwoorden van dergelijke klachten, verzoeken en bevelen. Dit houdt voor Verwerker in dat op het eerste daartoe strekkende verzoek van de Verantwoordelijke alle relevante informatie aan haar wordt verstrekt betreffende de aspecten van de door de Verwerker verrichte verwerking van Persoonsgegevens, zodat de Verantwoordelijke, mede aan de hand van die informatie, aan kan tonen dat Privacywetgeving of andere toepasselijke wetgeving wordt dan wel is nageleefd.

5.2. Voor zover mogelijk en rekening houdend met de aard van de verwerking, zal de Verwerker passende technische en organisatorische maatregelen implementeren voor de vervulling van zijn verplichtingen genoemd in dit Artikel 5.

6. Onderaanneming

6.1. De Verwerker kan zijn verplichtingen uit hoofde van deze Verwerkersovereenkomst slechts uitbesteden aan een derde partij met uitdrukkelijke voorafgaande schriftelijke toestemming van de Verantwoordelijke en alleen middels een schriftelijke overeenkomst met de onderaannemer (“Subverwerker”), welke overeenkomst dezelfde of zelfs strengere verplichtingen oplegt als aan de Verwerker onder deze Verwerkersovereenkomst dan wel uit de Privacywetgeving of andere toepasselijke wetgeving voortvloeit. Het is de (wettelijke) taak van de Verwerker om toe te zien op naleving daarvan door de Subverwerker.

6.2. De Verwerker blijft volledig aansprakelijk voor de nakoming van zijn verplichtingen uit hoofde van deze Verwerkersovereenkomst, met inbegrip van de door de onderaannemer verwerkte persoonsgegevens, indien de Verwerker gebruik maakt van onderaannemers.

De toestemming van Verantwoordelijke voor het uitbesteden van werkzaamheden aan een Subverwerker, zoals bedoeld in lid 1 van dit Artikel, laat onverlet dat Persoonsgegevens niet mogen worden verwerkt door die Subverwerker in een land buiten de Europese Economische Ruimte ("EER"), zonder daarvoor uitdrukkelijke voorafgaande schriftelijke toestemming van de Verantwoordelijke, zoals mede bedoeld in Artikel 2.7.

7. Vrijwaring en Boete

7.1. De Verwerker zal de Verantwoordelijke vrijwaren ten aanzien van alle schade die door de Verantwoordelijke of door haar groepsmaatschappijen wordt geleden of voortvloeit uit schending van deze Verwerkersovereenkomst door de Verwerker. Te denken valt hierbij aan een toerekenbare tekortkoming door Verwerker en/of diens onderaannemers (Subverwerkers) in de nakoming van zijn verplichtingen onder deze Verwerkersovereenkomst en/of enige schending door Verwerker en/of diens onderaannemers (Subverwerkers) van de Privacywetgeving of andere toepasselijke wetgeving op het gebied van verwerking van Persoonsgegevens. Voor de toepassing van dit Artikel betekent schade: i) boetes, dwangsommen en andere sancties die door een toezichthoudende autoriteit of andere overheidsinstantie worden opgelegd, ii) eventuele schadevergoeding die wordt geëist door derden of onderaannemers; en iv) redelijke kosten die verband houden met de tenuitvoerlegging van dit Artikel 7.

7.2. Partijen dragen zorg voor afdoende dekking van de aansprakelijkheid.

7.3. In geval van overtreding van een van de bepalingen van deze Verwerkersovereenkomst verbeurt Verwerker aan Verantwoordelijke een eenmalige, onmiddellijke en niet voor verrekening vatbare boete van EUR 10.000,- per overtreding alsmede een boete van 15% van voornoemd bedrag voor elke dag of gedeelte daarvan dat de overtreding voortduurt, een en ander onverminderd het recht van Verantwoordelijke op vergoeding van de door haar geleden en te lijden schade.

8. Audit en Controle

8.1. De Verwerker houdt gedetailleerde, nauwkeurige en actuele informatie bij met betrekking tot de verwerking van de Persoonsgegevens door hem in het kader van deze Verwerkersovereenkomst, waaronder met betrekking tot de verplichtingen en maatregelen op grond van de Artikelen 2.1, 3, 4, 5 en 6 ("**Bescheiden**"). Op verzoek van de Verantwoordelijke verstrekt de Verwerker deze Bescheiden aan de Verantwoordelijke.

8.2. Verantwoordelijke heeft het recht toe te (laten) zien op de naleving van de hiervoor onder Artikel 3 genoemde maatregelen. De Verwerker verstrekt de Verantwoordelijke, zijn daartoe gemachtigde vertegenwoordigers en/of de onafhankelijke auditor die door de Verantwoordelijke is aangewezen, zo vaak als Verantwoordelijke daar aanleiding toe ziet in het kader van de uitvoering van deze Verwerkersovereenkomst en bij (het vermoeden van) informatie- of privacy-incidenten, en met inachtneming van een redelijke termijn van kennisgeving: i) toegang tot de informatie, locaties en Bescheiden van de Verwerker; ii) redelijke bijstand en medewerking van het betrokken personeel van de Verwerker; en iii) redelijke faciliteiten op de locaties van de Verwerker om na te gaan of de Verwerker zijn verplichtingen uit hoofde van deze Verwerkersovereenkomst en de Privacywetgeving nakomt.

8.3. Verwerker zal eventuele door Verantwoordelijke naar aanleiding van dergelijke audits en controles in redelijkheid gegeven instructies tot aanpassing van het beveiligingsbeleid binnen een redelijke termijn opvolgen.

8.4. Elke partij draagt haar eigen kosten voor de in dit Artikel 8 beschreven audits en controles, tenzij blijkt dat de Verwerker een wezenlijke inbreuk heeft gepleegd op de bepalingen van deze Verwerkersovereenkomst, in welk geval de Verwerker alle kosten zal dragen, onverminderd andere rechten en rechtsmiddelen waarover de Verantwoordelijke beschikt.

9. Termijn en Beëindiging

9.1. Deze Verwerkersovereenkomst vangt aan vanaf datum van ondertekening door beide Partijen en blijft van kracht tot de beëindiging of afloop van de Hoofdovereenkomst.

9.2. Indien de Hoofdovereenkomst eindigt, eindigt deze Verwerkersovereenkomst automatisch; de Verwerkersovereenkomst kan niet tussentijds of separaat worden opgezegd.

9.3. Alle bepalingen van deze Verwerkersovereenkomst die uitdrukkelijk of impliciet zijn bedoeld om van kracht te blijven na beëindiging of afloop van deze Verwerkersovereenkomst, met inbegrip van de Artikelen 3.3 (geheimhouding), 4.2 (melden Beveiligingsincidenten), 7 (vrijwaring en boete), 8.1 (bijhouden van Bescheiden) en 10.1 (retour Persoonsgegevens) blijven volledig van kracht.

10. Overig

10.1. Na beëindiging of aflopen van deze Verwerkersovereenkomst, of op schriftelijk verzoek van de Verantwoordelijke, zal de Verwerker, op eventuele aanwijzing van de Verantwoordelijke binnen 30 dagen alle Persoonsgegevens retourneren aan Verantwoordelijke, en bestaande kopieën van alle bestaande exemplaren verwijderen.

10.2. Deze Verwerkersovereenkomst wordt beheerst door en geïnterpreteerd in overeenstemming met Nederlands recht. Elk geschil dat voortkomt uit deze Verwerkersovereenkomst of daarmee verband houdt (van contractuele of niet-contractuele aard) wordt uitsluitend voorgelegd aan de daartoe in de Hoofdovereenkomst aangewezen rechtbank of arbiter(s) of andere daartoe overeengekomen vorm van geschillenbeslechting, waarbij wordt opgemerkt dat Partijen te allen tijde nastreven een eventueel geschil eerst in onderling overleg op passende wijze op te lossen.

10.3. Wijzigingen van deze Verwerkersovereenkomst zijn slechts van kracht indien zij schriftelijk zijn vastgelegd en ondertekend door Partijen (of hun gemachtigde vertegenwoordigers).

Aldus overeengekomen en opgemaakt in tweevoud, van een paraaf voorzien op iedere pagina en ondertekend op [datum] te [plaats],

[verantwoordelijke]	[Verwerker]
[tekeningsbevoegde namens verantwoordelijke]	[tekeningsbevoegde namens verwerker]

ANNEX 1

Verwerker verwerkt de Persoonsgegevens [*Maak een keuze*: nader beschreven in de Hoofdovereenkomst / hieronder nader uiteengezet].

[In te vullen met verwijzingen naar de overeenkomstige Artikelen in de Hoofdovereenkomst]

Type/Categorie Betrokkene	**Beschrijving van persoonsgegevens** (volledige lijst)	**Soort verwerking van persoons-gegevens**	**De geografische locatie van de verwerking**	**Doel(einden) van de verwerking van persoons-gegevens**	**Voorafgaande toestemming onderaannemers "Subverwerkers"**
Om wie gaat het	Welke soort gegevens, zie bijlage 1	*[beschrijving van de verwerkings-activiteiten / korte toelichting op de diensten]*	*[beschrijving van de locatie, land, adres]*	*Patiëntendossier aanleggen en onderhouden.*	*[lijstje met onderaannemers die worden ingeschakeld door Verwerker en de vermelding of er al dan niet voorafgaand uitdrukkelijk schriftelijk toestemming is gegeven]*

ANNEX 2

1. Wettelijke voorschriften

De Verwerker zal eventuele specifieke veiligheidsbepalingen identificeren en zorgdragen voor de naleving van dergelijke veiligheidsbepalingen met betrekking tot de verwerking van Persoonsgegevens.

2. Praktische veiligheidsmaatregelen

In overeenstemming met haar verplichtingen uit hoofde van Artikel 3.2 van de Verwerkersovereenkomst zal de Verwerker naar behoren rekening houden met de volgende soorten veiligheidsmaatregelen om een naar risico aangepast beveiligingsniveau te garanderen:

- de pseudonimisering en versleuteling van Persoonsgegevens;
- Fysieke beveiliging;
- Toegangscontrole;
- Beveiliging en *Privacy Enhancing Technologies*;
- Bewustmaking, opleiding en veiligheidscontroles met betrekking tot personeel;
- Incident/Response management/bedrijfscontinuïteit; en
- *Audit controls/Due Diligence*.

3. Veiligheidsbeleid en -instructies

De Verantwoordelijke kan de Verwerker nadere instructies en policies verstrekken met betrekking tot dergelijke technische en organisatorische beveiligingsmaatregelen.

ANNEX 3

Meld Beveiligingsincidenten, als bedoeld in Artikel 4.2 van de Verwerkersovereenkomst, onverwijld bij Verantwoordelijke, tenzij uitdrukkelijk anders vermeld, via de onderstaande contactgegevens. Als het primaire contact niet binnen één uur reageert kunt u contact opnemen met een van de twee andere contacten. Ook de contactgegevens van Verwerker staan hieronder ter volledigheid vermeld.

Primair contactpersoon *Verantwoordelijke*

Naam	
Functie	
E-mail	
Telefoon	

Verdere contactpersonen *Verantwoordelijke*

Naam	
Functie	
E-mail	
Telefoon	

Naam	
Functie	
E-mail	
Telefoon	

Primair contactpersoon *Verwerker*

Naam	
Functie	
E-mail	
Telefoon	

Verdere contactpersonen *Verwerker*

Naam	
Functie	
E-mail	
Telefoon	

Naam	
Functie	
E-mail	
Telefoon	

Geef in ieder geval de volgende informatie door bij het melden van een Beveiligingsincident:

- Samenvatting van het Beveiligingsincident (incl. datum en tijdstip, geschat aantal bestanden, geschat aantal betrokkenen, de (mogelijk) getroffen persoonsgegevens, soort beveiligingsincident, de geconstateerde en/of vermoedelijke gevolgen voor betrokkene(en) van het incident);

- Getroffen technische en organisatorische maatregelen om het Beveiligingsincident aan te pakken, maatregelen om de mogelijke negatieve gevolgen ervan te beperken en verdere Beveiligingsincidenten te voorkomen; en

- Verdere (relevante) informatie die Verantwoordelijke nodig kan hebben om te voldoen aan de wettelijke verplichtingen ten aanzien van Beveiligingsincidenten, waaronder in ieder geval het (kunnen) doen van een eventuele melding bij de Autoriteit Persoonsgegevens en/of het informeren van betrokkene(n).