# Verwerkersovereenkomst Brancheorganisaties Zorg

**Verenigd in**

Uitleg bij deze verwerkersovereenkomst kunt u hier vinden: https://www.brancheorganisatieszorg.nl/wp-content/uploads/2023/03/Toelichting-BoZ-verwerkersovereenkomst-2022.pdf

**VERWERKERSOVEREENKOMST**

DE ONDERGETEKENDEN:

1. Verwerkingsverantwoordelijke zoals beschreven in de Hoofdovereenkomst met kenmerk offertenummer invoeren; en

2. Triaspect B.V., gevestigd aan de Groenestraat 72 te Nijmegen en ingeschreven in het register van de Kamer van Koophandel onder nummer 52835561 in deze rechtsgeldig vertegenwoordigd door Pim Südmeier, directeur (hierna: "**Verwerker**");

Hierna gezamenlijk ook aan te duiden als: "Partijen" en afzonderlijk als "Partij".

OVERWEGENDE DAT:

(a) Verwerker diensten verricht ten behoeve van Verwerkingsverantwoordelijke, zoals beschreven in de Hoofdovereenkomst hierboven genoemd waarbij deze Verwerkersovereenkomst een bijlage is.
(b) De diensten meebrengen dat Persoonsgegevens worden verwerkt.
(c) Verwerker de betreffende gegevens louter in opdracht van Verwerkingsverantwoordelijke verwerkt en niet voor eigen doeleinden.
(d) Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 (hierna: "AVG") op deze verwerking van toepassing is.
(e) Partijen in 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 Verwerkersovereenkomst(en) van gelijke strekking tussen Partijen vervangt.
(g) De Brancheorganisaties Zorg met deze Verwerkersovereenkomst een standaard hebben willen opstellen.

VERKLAREN TE ZIJN OVEREENGEKOMEN ALS VOLGT:

**Artikel 1. Definities**

1.1. Termen met een hoofdletter die in deze Verwerkersovereenkomst worden gebruikt en die hierin niet worden gedefinieerd, hebben de betekenis die is uiteengezet in de AVG (waaronder Persoonsgegevens, Betrokkene, Verwerkingsverantwoordelijke en Verwerker).

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

a) Inbreuk
i een onderzoek naar of beslaglegging door overheidsfunctionarissen op de

| | | |
|---|---|---|
| | | Persoonsgegevens of een vermoeden dat dit gaat plaatsvinden;<br>ii een Inbreuk in verband met Persoonsgegevens als bedoeld in artikel 4 onder 12 AVG; |
| b) | Medewerker | een bij de uitvoering van deze Verwerkersovereenkomst betrokken natuurlijke persoon die werkzaam is bij of voor een van de Partijen. |
| c) | Hoofdovereenkomst | de Hoofdovereenkomst(en) betreffende de levering van producten en/of diensten. waarvan deze Verwerkersovereenkomst als Bijlage onderdeel uitmaakt. |
| d) | Verzoek van Betrokkene | Een klacht over de verwerking dan wel een verzoek tot uitoefening van de rechten van Betrokkene zoals omschreven in Hoofdstuk III van de AVG. |

1.3. Waar in deze Verwerkersovereenkomst naar bepaalde normen wordt verwezen (zoals NEN 7510) wordt daarmee steeds gedoeld 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 en beschrijving Bijlagen**

2.1. Deze Verwerkersovereenkomst betreft de verwerking van Persoonsgegevens door Verwerker in opdracht van de Verwerkingsverantwoordelijke in het kader van de uitvoering van de Hoofdovereenkomst.

2.2. Onderdeel van deze Verwerkersovereenkomst zijn de volgende Bijlagen:
   a) Bijlage 1: Omschrijving van de verwerking
   b) Bijlage 2: Beveiliging Persoonsgegevens
   c) Bijlage 3: Contactinformatie mbt. verwerking/Inbreuken/Verzoeken van Betrokkenen.

2.3. Deze Verwerkersovereenkomst maakt onverbrekelijk deel uit van de Hoofdovereenkomst. Voor zover het bepaalde in de Verwerkersovereenkomst strijdig is met het bepaalde in de Hoofdovereenkomst, prevaleert het bepaalde in de Verwerkersovereenkomst.

**Artikel 3. Uitvoering verwerking**

3.1. Verwerker garandeert dat hij ten behoeve van Verwerkingsverantwoordelijke uitsluitend Persoonsgegevens zal verwerken voor zover:
   a) dit noodzakelijk is voor de uitvoering van de Hoofdovereenkomst (binnen de gespecificeerde omschrijving in Bijlage 1); of
   b) Verwerkingsverantwoordelijke daartoe nadere schriftelijke instructies heeft gegeven.

3.2. Verwerker zal alle redelijke instructies 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. 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 de 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.

3.4. 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 en overige wet- en regelgeving.

3.5. Verwerker zal, tenzij hij hiervoor uitdrukkelijke voorafgaande schriftelijke toestemming heeft verkregen van Verwerkingsverantwoordelijke, geen Persoonsgegevens verwerken of door derden laten verwerken in landen buiten de Europese Economische Ruimte (“EER”).

3.6. Verwerker waarborgt dat Medewerkers een geheimhoudingsovereenkomst hebben getekend dan wel garandeert dat Medewerkers geheimhouding zullen betrachten ten aanzien van de verwerking van de Persoonsgegevens.

**Artikel 4. Beveiliging Persoonsgegevens en controle (versie gezondheidsgegevens) [Doorhalen indien niet van toepassing]**

4.1. Verwerker zal aantoonbaar passende en doeltreffende technische en organisatorische beveiligingsmaatregelen nemen die, gezien de huidige stand der techniek en de daarmee gemoeide kosten, afgestemd zijn op de (in Bijlage 1 gespecificeerde) aard van de te verwerken Persoonsgegevens, ter bescherming van de Persoonsgegevens tegen verlies, onbevoegde kennisname, verminking of enige vorm van onrechtmatige verwerking, alsmede om de (tijdige) beschikbaarheid en integriteit van de gegevens te garanderen. In deze beveiligingsmaatregelen zijn de mogelijk in de Hoofdovereenkomst reeds beschreven maatregelen begrepen.

4.2. Verwerker beschikt over ISO 27001-certificering, vergelijkbare certificering of werkt aantoonbaar in overeenstemming met ISO 27001 en heeft een passend, geschreven beveiligingsbeleid geïmplementeerd voor de verwerking van Persoonsgegevens, waarin in ieder geval de in het eerste lid van dit artikel 4 genoemde maatregelen uiteengezet zijn.

4.3. Verwerker beschikt over NEN 7510-certificering of werkt aantoonbaar in overeenstemming met NEN 7510 en heeft een passend, geschreven beveiligingsbeleid geïmplementeerd voor de verwerking van Persoonsgegevens. Verwerker voldoet aantoonbaar (indien van toepassing) aan de veiligheidseisen voor netwerkverbindingen zoals beschreven in NEN 7512 en aan de eisen ten aanzien van logging zoals beschreven in NEN 7513.

4.4. Verwerker zal op eerste verzoek van Verwerkingsverantwoordelijke een (kopie van een) door een onafhankelijke en ter zake deskundige derde afgegeven geldig certificaat overleggen alsmede de verklaring van toepasselijkheid, indien deze daarover beschikt, of een Third Party Memorandum (TPM), waaruit volgt dat Verwerker de verplichtingen uit dit artikel naleeft.

4.5. Verwerker laat zelf regelmatig interne en/of externe audits uitvoeren met betrekking tot de naleving van bovengenoemde normen.

4.6. Verwerkingsverantwoordelijke heeft het recht toe te (laten) zien op de naleving van de hiervoor onder artikel 4.1 tot en met 4.3 genoemde maatregelen naar aanleiding van (vermoeden van) informatiebeveiligings- of privacy-Inbreuken. Verwerker en Verwerkingsverantwoordelijke bepalen in gezamenlijk wanneer en door welke onafhankelijke derde partij de controle wordt uitgevoerd. Verwerker zal eventuele door Verwerkingsverantwoordelijke naar aanleiding van een dergelijk onderzoek in redelijkheid gegeven instructies tot aanpassing van het beveiligingsbeleid binnen een redelijke termijn opvolgen.

4.7. Partijen erkennen dat beveiligingseisen voortdurend veranderen en dat een effectieve beveiliging frequente evaluatie en regelmatige verbetering van verouderde beveiligingsmaatregelen vereist. Verwerker zal daarom de maatregelen zoals geïmplementeerd op basis van dit artikel 4 periodiek evalueren en, waar nodig, de maatregelen verbeteren om te blijven voldoen aan de verplichtingen onder dit artikel 4. Het voorgaande laat de instructiebevoegdheid van Verwerkingsverantwoordelijke om zo nodig aanvullende maatregelen te (doen) treffen onverlet.

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

5.1. Verwerker zal actief monitoren op Inbreuken op de beveiliging en over de resultaten van de monitoring in overeenstemming met dit artikel 5 rapporteren aan Verwerkingsverantwoordelijke.

5.2. Wanneer zich een Inbreuk voordoet of heeft voorgedaan, is Verwerker verplicht de contactpersoon van Verwerkingsverantwoordelijke genoemd in Bijlage 3 daarvan onmiddellijk, doch uiterlijk binnen 24 uur nadat Verwerker er kennis van heeft genomen, in kennis te stellen en daarbij alle relevante informatie te verstrekken over:

1) de aard van de Inbreuk;
2) de (mogelijk) getroffen Persoonsgegevens;
3) de geconstateerde en de vermoedelijke gevolgen van de Inbreuk; en
4) de maatregelen die getroffen zijn of zullen worden om de Inbreuk 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 de Inbreuk zo snel mogelijk te herstellen dan wel de verdere gevolgen zoveel mogelijk te beperken. Verwerker treedt zo snel als mogelijk, doch binnen 24 uur, in overleg met Verwerkingsverantwoordelijke teneinde hierover nadere afspraken te maken.

5.4. Verwerker zal Verwerkingsverantwoordelijke te allen tijde zijn medewerking verlenen en zal de instructies van Verwerkingsverantwoordelijke opvolgen en deugdelijk onderzoek naar de Inbreuk verrichten. Verwerker stelt daarover een rapportage op, inclusief een correcte respons en passende vervolgstappen. Deze rapportage deelt Verwerker zo spoedig mogelijk met Verwerkingsverantwoordelijke zodat deze tijdig de Autoriteit Persoonsgegevens (hierna: AP) en/of de Betrokkene kan informeren. Het melden van een Inbreuk aan de AP en/of Betrokkene kan alleen gedaan worden door de Verwerkingsverantwoordelijke.

5.5. Meldingen met betrekking tot Inbreuken en Verzoeken van Betrokkenen worden gedaan aan de contactpersoon van Verwerkingsverantwoordelijke zoals beschreven in Bijlage 3.
5.6. Het is Verwerker niet toegestaan informatie te verstrekken over Inbreuken aan Betrokkenen of andere derde partijen, behoudens voor zover Verwerker daartoe wettelijk verplicht is of Partijen anderszins zijn overeengekomen.
5.7. Indien en voor zover Partijen zijn overeengekomen dat Verwerker in relatie tot een Inbreuk rechtstreeks contact onderhoudt met autoriteiten anders dan de AP, of andere derde partijen, dan houdt de Verwerker de Verwerkingsverantwoordelijke daarvan voortdurend op te hoogte.

**Artikel 6. Medewerkingsverplichtingen**

6.1. De AVG en overige wetgeving kent aan de Betrokkene bepaalde rechten toe. Verwerker zal zijn volledige en tijdige medewerking verlenen aan Verwerkingsverantwoordelijke bij de nakoming van de op Verwerkingsverantwoordelijke rustende verplichtingen voortvloeiend uit deze rechten.
6.2. Een door Verwerker ontvangen Verzoek van een Betrokkene met betrekking tot verwerking van Persoonsgegevens wordt door Verwerker zo snel als mogelijk, doch binnen 24 uur, doorgestuurd naar Verwerkingsverantwoordelijke.
6.3. Op het eerste daartoe strekkende verzoek van Verwerkingsverantwoordelijke zal Verwerker aan Verwerkingsverantwoordelijke alle relevante informatie verstrekken betreffende de aspecten van de door hem verrichte verwerking van Persoonsgegevens zodat Verwerkingsverantwoordelijke, mede aan de hand van die informatie, aan kan tonen dat zij de toepasselijke (privacy) wetgeving naleeft.
6.4. Verwerker zal voorts op verzoek van Verwerkingsverantwoordelijke alle noodzakelijke bijstand verlenen bij de nakoming van de op grond van de toepasselijke privacywetgeving op Verwerkingsverantwoordelijke rustende wettelijke verplichtingen, zoals het uitvoeren van een gegevensbeschermingseffectbeoordeling (DPIA).

**Artikel 7. Inschakeling subverwerkers**

7.1. Verwerker zal zijn activiteiten die bestaan uit het verwerken van Persoonsgegevens of vereisen dat Persoonsgegevens verwerkt worden, niet uitbesteden aan een subverwerker zonder drie maanden van te voren dat mede te delen aan Verwerkingsverantwoordelijke en de Verwerkingsverantwoordelijke de gelegenheid te geven om eventuele bezwaren aan de Verwerker kenbaar te maken. Indien Verwerkingsverantwoordelijke bezwaren heeft, zal Verwerker redelijke inspanningen leveren om de bezwaren van de Verwerkingsverantwoordelijke op te lossen of om de levering van de diensten zoals genoemd in de Hoofdovereenkomst - zonder daaraan afbreuk te doen - aan te passen om verwerking van Persoonsgegevens door de voorgestelde (nieuwe) subverwerker te voorkomen.
7.2. Indien de Verwerker de bezwaren van de Verwerkingsverantwoordelijke niet kan oplossen of de levering van de diensten niet kan aanpassen om de verwerking van Persoonsgegevens door de voorgestelde subverwerker te voorkomen, kan de Verwerkingsverantwoordelijke de Hoofdovereenkomst opschorten of geheel of gedeeltelijk beëindigen, met inachtneming van een opzegtermijn van zes maanden, gerekend vanaf de einddatum van de bezwaartermijn. Gedurende een schorsing van de Hoofdovereenkomst vanwege bezwaar tegen een (nieuwe) subverwerker en vanaf de einddatum van de Hoofdovereenkomst is de

Verwerkingsverantwoordelijke niet verplicht om de Verwerker enige vergoeding op grond van de Hoofdovereenkomst of anderszins of enige schadevergoeding te betalen.

7.3. Artikel 7.1 is niet van toepassing op de in Bijlage 1 vermelde subverwerkers.

7.4. Verwerker zal aan deze subverwerker minstens dezelfde verplichtingen opleggen als voor hemzelf uit deze Verwerkersovereenkomst en de wet voortvloeien. Verwerker zal deze afspraken schriftelijk vastleggen en zal toezien op de naleving daarvan door de subverwerker. Verwerker zal Verwerkingsverantwoordelijke op verzoek afschrift verstrekken van de met de subverwerker gesloten verwerkersovereenkomst.

7.5. Verwerker blijft volledig aansprakelijk jegens Verwerkingsverantwoordelijke voor de gevolgen van het uitbesteden van werkzaamheden aan een subverwerker. Voor de inzet van subverwerkers buiten de EER is toestemming vereist in overeenstemming met artikel 3.5 van deze Verwerkersovereenkomst.

**Artikel 8. Kosten**

8.1. De kosten voor de verwerking van gegevens die inherent zijn aan de normale uitvoering van de Verwerkersovereenkomst en de uitoefening van rechten van Betrokkenen, worden geacht besloten te liggen in de op grond van de Hoofdovereenkomst reeds verschuldigde vergoedingen.

**Artikel 9. Duur en beëindiging**

9.1. Deze Verwerkersovereenkomst gaat in op de datum van ondertekening en de duur van deze Verwerkersovereenkomst is gelijk aan de duur van de Hoofdovereenkomst inclusief eventuele verlengingen daarvan.

9.2. De Verwerkersovereenkomst maakt na ondertekening ervan door beide Partijen integraal en onverbrekelijk 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, tenzij Partijen in voorkomend geval anders overeenkomen.

9.3. 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 verplichtingen behoren bijvoorbeeld die welke voortvloeien uit de bepalingen betreffende geheimhouding, aansprakelijkheid, geschillenbeslechting en toepasselijk recht.

9.4. 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 deze Verwerkersovereenkomst [en de daarmee samenhangende Hoofdovereenkomst] zonder rechterlijke tussenkomst met onmiddellijke ingang te beëindigen indien:

a) de andere Partij wordt ontbonden of anderszins ophoudt te bestaan;
b) de andere Partij aantoonbaar ernstig tekortschiet in de nakoming van de verplichtingen die voortvloeien uit deze Verwerkersovereenkomst en die toerekenbare tekortkoming niet binnen 30 dagen is hersteld na een daartoe strekkende schriftelijke ingebrekestelling;
c) een Partij in staat van faillissement wordt verklaard of surseance van betaling aanvraagt.

9.5. 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.

9.6. 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 de wet en/of de rechtspraak aan de verwerking van de Persoonsgegevens worden gesteld.

9.7. Verwerker dient Verwerkingsverantwoordelijke zo spoedig mogelijk te informeren over een voorgenomen overname of eigendomsoverdracht. Verwerkingsverantwoordelijke heeft het recht bij zwaarwegende bezwaren tegen de verandering van eigenaar de Hoofdovereenkomst te beëindigen zonder schadeplichtig te zijn.

9.8. Het is Verwerker niet toegestaan om zonder uitdrukkelijke en schriftelijke toestemming van Verwerkingsverantwoordelijke deze Verwerkersovereenkomst en de rechten en plichten die samenhangen met deze Verwerkersovereenkomst over te dragen aan een derde partij.

9.9. De verplichtingen uit deze Verwerkersovereenkomst duren voort zolang de Verwerker Persoonsgegevens van Verwerkingsverantwoordelijke verwerkt, ook nadat de Verwerker is opgehouden de in de Hoofdovereenkomst opgedragen zorg, diensten en/of faciliteiten ten behoeve van Verwerkingsverantwoordelijke te verlenen.

**Artikel 10. Bewaartermijnen, teruggave en vernietiging van Persoonsgegevens**

10.1. Verwerker bewaart de Persoonsgegevens niet langer dan strikt noodzakelijk, waaronder begrepen de wettelijke bewaartermijnen of een eventueel tussen Partijen gemaakte afspraak over bewaartermijnen zoals vastgelegd in Bijlage 1. In geen geval bewaart Verwerker de Persoonsgegevens langer dan tot het einde van deze Verwerkersovereenkomst. Verwerkingsverantwoordelijke bepaalt of en zo ja hoe lang gegevens bewaard moeten blijven.

10.2. Bij beëindiging van de Verwerkersovereenkomst, of indien van toepassing aan het einde van de overeengekomen bewaartermijnen, of op schriftelijk verzoek van Verwerkingsverantwoordelijke zal Verwerker, tegen redelijke kosten, naar keuze van Verwerkingsverantwoordelijke, de Persoonsgegevens definitief (doen) vernietigen of teruggeven aan Verwerkingsverantwoordelijke. Op verzoek van Verwerkingsverantwoordelijke verstrekt Verwerker bewijs van het feit dat de gegevens onherroepelijk zijn vernietigd of verwijderd. Eventuele teruggave van de gegevens zal in een algemeen gangbaar, gestructureerd en gedocumenteerd gegevensformaat langs elektronische weg plaatsvinden. Indien teruggave, definitieve vernietiging of verwijdering niet mogelijk is, 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.

**Artikel 11. Slotbepalingen**

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

11.2. Op deze Verwerkersovereenkomst is Nederlands recht van toepassing.

11.3. Geschillen over of in verband met deze Verwerkersovereenkomst worden uitsluitend voorgelegd aan de daartoe in de Hoofdovereenkomst aangewezen rechtbank of arbiter(s).

**Door Triaspect toegevoegd: Door de offerte te ondertekenen met het kenmerk zoals genoemd in punt 1 bij Verwerkingsverantwoordelijke wordt deze Verwerkersovereenkomst automatisch door verwerkingsverantwoordelijke geaccepteerd. Dit is ook opgenomen in de bovengenoemde offerte.**

**Bijlage 1: Omschrijving van de verwerking**

Omschrijving van activiteiten en/of diensten, omvang en algemeen doel van de verwerking (benoem het aantal Persoonsgegevens/Betrokkenen).
Let op! Deze bijlage is ingevuld door Triaspect. De verantwoordelijkheid van de doelbinding, de grondslag etc ligt bij de verwerkingsverantwoordelijke. U kunt hier zelf uw doelbinding, grondslag etc formuleren en aangeven welke gegevens wel en niet verwerkt moeten of mogen worden.

Noem Hoofdovereenkomst: Voor het nummer van de hoofdovereenkomst verwijzen we naar de overeenkomst die genoemd is bij Verwerkingsverantwoordelijke onder punt 1 van de Verwerkersovereenkomst waarvan dit de eerste bijlage is.

*Geef een omschrijving van activiteiten en/of diensten:*
Leveren van een SaaS-oplossing ten behoeve van melden en analyseren van incidenten, klachten en andere gebeurtenissen, risico's, audits, verbeteracties, RI&E, etc.

*Wat is het algemeen doel van de verwerking:*
De veiligheid van zorg voor client en medewerker te bewaren en waar nodig te verbeteren.

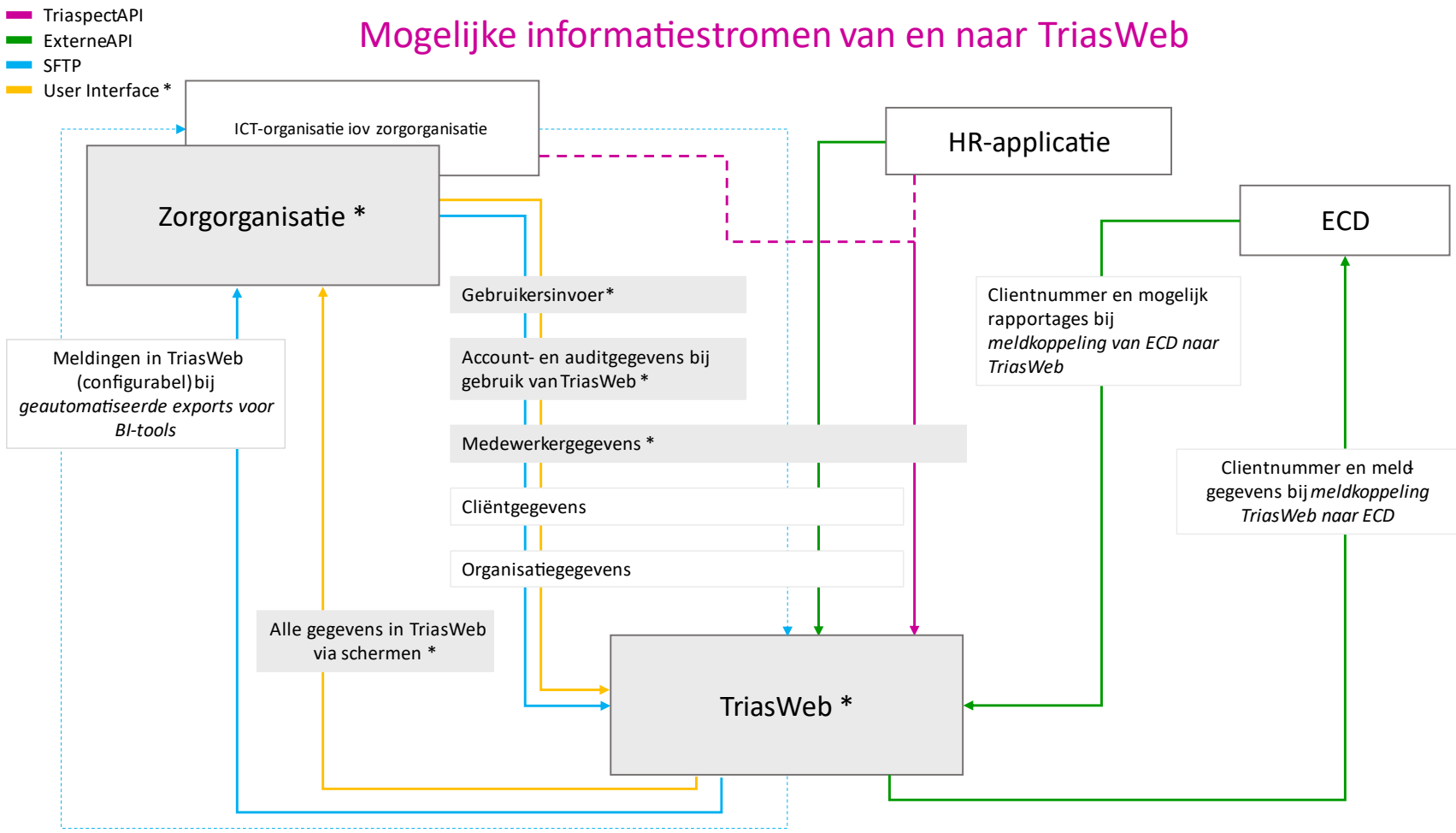
Aangezien Verwerkingsverantwoordelijke heeft gekozen om daarvoor TriasWeb in te zetten is het volgende nodig:

- De inrichting, beschikbaarstelling, instandhouding, werking, beveiliging en betrouwbaarheid van TriasWeb en de daaronder vallende functionaliteiten.
- Het juist en volgens afspraken afleveren van berichten
- Het tonen van Persoonsgegevens in TriasWeb en de daarbij behorende functionaliteiten
- Het verminderen van de administratielast van medewerkers van wanneer zowel een Incidentmelding in TriasWeb als een rapportage in ECD noodzakelijk zijn.
- De goede werking van een toekomstige nieuwe functionaliteit binnen TriasWeb mits deze nieuwe functionaliteit verenigbaar is met de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG).

*Categorieën van betrokkenen:*

- Gebruikers van het systeem (over het algemeen medewerkers, mogelijk ook derden)
- Betrokkenen (over het algemeen cliënten en medewerkers, mogelijk ook derden)

*Verwerking van persoonsgegevens. Onderdelen zonder asterisk zijn optioneel en afhankelijk van door de zorgorganisatie gekozen modules en methodes.*




* Noodzakelijke informatiestromen en onderdelen. Overige stromen en onderdelen zijn optioneel in te zetten.

| Verwerking | Soort Persoonsgegevens | Categorieën van Betrokkenen | Doeleinden van de verwerking | Grondslag van de verwerking | Doorgifte buiten de EER | Afspraken bewaartermijnen | Afspraken verwijderprocedure |
|---|---|---|---|---|---|---|---|
| Noem de verwerking (bijvoorbeeld hosting, transfer, onderhoud, of naam van de applicatie). | Benoem de Persoonsgegevens (b.v. NAW, BSN, gegevens over gezondheid, etc.)<br><br>**Persoonsgegevens met asterisk(*) zijn noodzakelijk, overige persoonsgegevens zijn afhankelijk van de aangeschafte modules.** | Benoem Betrokkenen (patiënten, Medewerkers, studenten, etc.) | Benoem het doel van de verwerking. | Benoem de grondslag waarop de verwerking plaatsvindt. | Indien ja, benoem opslag/ verwerking buiten de EER en vermeld land, instrument waaronder doorgifte kan plaatsvinden (hoofdstuk V AVG) en aanvullende maatregelen. | Benoem afspraken bewaartermijnen. | Benoem de verwijderprocedure. |
| TriasWeb-inloggen | E-mailadres * | Gebruiker (=medewerkers, mogelijk ook derden) | Inloggen in de software. Communicatie over meldingen en verbeteracties in TriasWeb. | Wkkgz art. 7 en 9 *<br>Arbowet **<br>Contract *** | Nee | Gegevens worden op de systemen van Triaspect bewaard zolang deze overeenkomst geldt of totdat Verwerkingsverantwoordelijke opdracht geeft tot vernietiging van (een deel) van de gegevens. | Drie weken na vervallen overeenkomst worden alle gegevens definitief verwijderd. Of Verantwoordelijke geeft opdracht tot vernietiging van (een deel) van de gegevens. |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| TriasWeb-gebruikersbeheer en identificatie | Unieke code (personeelsnummer) | Gebruiker | Referentie voor bijwerken gebruikersgegevens door importmodule in TriasWeb. | idem | idem | idem | idem |
| TriasWeb-gebruikersbeheer en identificatie | Naam | Gebruiker | Gebruiksvriendelijkheid van gebruikerselectiefunctionaliteit in TriasWeb. | idem | idem | idem | idem |
| TriasWeb-gebruikersbeheer en identificatie | Gekoppelde Organisatorische Eenheden | Gebruiker | Scope bepalen van autorisatie van gebruiker. | idem | idem | idem | idem |
| TriasWeb-medewerkergerelateerde meldingen | Gezondheidsgegevens, gegevens over psychisch en fysiek welbevinden | Gebruiker | Interpretatie door gebruikers met analyserol in de software. | idem | idem | idem | idem |
| TriasWeb-cliëntbeheer en identificatie | Unieke code (cliëntnummer) | Cliënten | Referentie voor bijwerken cliëntgegevens door importmodule in TriasWeb. | idem | idem | idem | idem |
| TriasWeb-cliëntbeheer en identificatie | Naam | Cliënten | Gebruiksvriendelijkheid van cliëntselectiefunctionaliteit in TriasWeb. | idem | idem | idem | idem |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| TriasWeb-cliëntbeheer en identificatie | Geboortedatum | Cliënten | Gebruiksvriendelijkheid van cliëntselectiefunctionaliteit in TriasWeb. | idem | idem | idem | idem |
| TriasWeb-cliëntbeheer en identificatie | Geslacht | Cliënten | Gebruiksvriendelijkheid van cliëntselectiefunctionaliteit in TriasWeb. | idem | idem | idem | idem |
| Triasweb-Autorisatie scope | Gekoppelde Organisatorische Eenheden | Cliënten | Zichtbaarheid bepalen van individuele cliënt (en meldingen) voor individuele gebruiker. | idem | idem | idem | idem |
| TriasWeb-cliëntgerelateerde meldingen | Gezondheidsgegevens, gegevens over psychisch en fysiek welbevinden | Cliënten | Interpretatie door gebruikers met analyserol in de software. | idem | idem | idem | idem |
| TriasWeb-meldingen met betrokken en | Gebruikersinvoer *. Vermoedelijk naam, gezondheidsgegevens, gegevens over psychisch en fysiek welbevinden | Derden betrokken bij incident | Interpretatie door gebruikers met analyserol in de software. | idem | idem | idem | idem |

* = Vanuit opdrachtgever voor clientgebonden meldingen

** = Vanuit opdrachtgever voor RI&E

*** = Vanuit verwerker volgens AVG

NB: aangezien TriasWeb in grote mate door de beheerder bij de zorginstelling in te richten is en het formulieren met open tekstvakken bevat, is het niet exact te voorspellen welke gegevens verwerkt worden. Bovenstaande tabel geeft een indicatie van de gegevens die over het algemeen in TriasWeb worden opgeslagen. Slechts de gegevens met een asterisk zijn noodzakelijk om TriasWeb te kunnen draaien.

**Overige gegevens**

| Type gegevens | Gegevens | Doel |
|---|---|---|
| **Accountgegevens *** | Inlognaam/e-mailadres | Inloggen met persoonlijk account. |
| | Wachtwoord (onomkeerbaar versleuteld) | Inloggen met persoonlijk account. Verlegd naar zorgorganisatie bij gebruik van SSO. |
| | Inlogpogingen | Beveiligingseisen Triaspect. |
| **Logging *** | Handelingen in TriasWeb | Logging ten behoeve van informatievoorziening bij en analyse van informatie-incidenten. |
| **Meldingsgegevens *** | Relatie van gebruiker tot meldingen en/of verbeteracties | Communicatie vanuit TriasWeb over meldingen en verbeteracties. |
| **Onbekend** | De software bevat vrijwel altijd een of meer open tekstvelden. Het is niet mogelijk om te voorspellen welke gegevens daarin opgenomen worden door gebruikers | Specificatie van antwoorden in meldformulieren en verbeteracties. |

## Subverwerkers

| Subverwerker | Beschrijving dienst en Persoonsgegevens | Gegevens buiten de EER | Verwerkers-overeenkomst |
|---|---|---|---|
| CJ2 Hosting B.V.<br>De Deimten 11<br>9747AV Groningen<br>(NEN 7510-gecertificeerd) | CJ2 is onze hostingpartner. Zij zorgen voor dat onze hardware in twee datacenters (QTS en North C) beschikbaar en bereikbaar is. Deze datacenters zijn beveiligde zones. Beide zijn ISO 27001-gecertificeerd. | Nee | Nee, SLA. |

## Toelichting:

**Persoonsgegevens** gaan over iemand (of zijn tot iemand te herleiden). Elk gegeven over een geïdentificeerde of identificeerbare natuurlijke persoon is een persoonsgegeven. De identificatie kan bijvoorbeeld gebeuren aan de hand van een identificatiemiddel, zoals een naam, een identificatienummer, locatiegegevens, een online identificerende variabele of andere elementen die kenmerkend zijn. Hierbij kunt u denken aan fysieke, fysiologische, genetische, psychische, economische, culturele of sociale elementen.

Elke **verwerking** moet één of meerdere welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde **doeleinden** hebben. Het gaat hierbij om het doel of de doelen waarvoor de Persoonsgegevens zijn verkregen/verzameld. Maak het **verwerkingsdoel/**de **verwerkingsdoelen** zo concreet mogelijk.

**Grondslagen** voor verwerking Persoonsgegevens: Toestemming Betrokkene / Noodzakelijk voor uitvoering van een overeenkomst / Wettelijke verplichting / Beschermen van vitale belangen van de Betrokkene / Taak van algemeen belang of uitoefening van het openbaar gezag / Gerechtvaardigde belangen van de Verwerkingsverantwoordelijke of van een derde.

**Bijlage 2: Beveiliging Persoonsgegevens**

Middels deze bijlage dient Verwerker aan te tonen welke maatregelen Verwerker geïmplementeerd heeft om de Persoonsgegevens veilig te verwerken.

Indien Verwerker beschikt over relevante **certificering** wat betreft informatiebeveiliging (**ISO 27001** en voor zorgprocessen aangevuld met **NEN 7510**), verzoeken wij kopieën hiervan als bijlage toe te voegen en daarbij tevens de bijbehorende **Verklaring van Toepasselijkheid (VvT)** (welke maatregelen zijn er wel of niet geïmplementeerd?) en **scopeomschrijving** (waarop is de certificering van toepassing?) aan te leveren.

Verwerker beschikt verwerker over de volgende certificering (kopieën, VvT en scopebeschrijving zijn bijgevoegd als bijlage bij deze Verwerkersovereenkomst): NEN 7510

TriasWeb (onderhoud, beheer en hosting) is gecertificeerd volgens NEN7510.

1. Hardware
    a. Het serverpark van Triaspect is ondergebracht in twee datacenters.
    b. Alle onderdelen in het serverpark (servers, switches, firewalls, stroomvoorziening en bekabeling) zijn redundant en operationeel aanwezig.
    c. Triaspect is de enige gebruiker van de hardware waarop TriasWeb en aanverwante software draait.
    d. Fysieke toegang tot de serverruimte in het datacenter wordt afgedwongen met biometrische authenticatie.
    e. Fysieke toegang tot de serverkast is voorbehouden aan Triaspectmedewerkers die belast zijn met het beheer van de servers.
2. Serversoftware
    a. Alle software op de servers in het Triaspect serverpark is volledig in beheer van Triaspect.
    b. De serversoftware is slechts toegankelijk voor Triaspectmedewerkers die belast zijn met het softwarematig beheer van de servers.
    c. Logging met betrekking tot toegang en ondernomen acties wordt bijgehouden en volgens standaarden bewaard.
3. TriasWeb
    a. TriasWeb kent geen anonieme inlog-mogelijkheid: voor de toegang tot TriasWeb is altijd een gebruikersnaam en wachtwoord nodig.
    b. Deze inlog kan geschieden via het TriasWeb inlogportaal of via het inlogportaal van de klant, door middel van Single Sign-On.
    c. Verwerker stelt standaard tweestapsverificatie in voor alle gebruikers. Verwerkingsverantwoordelijke kan dit aanpassen. Tweestapsverificatie voor beheerders staat altijd aan en kan niet uitgeschakeld worden. Tweestapsverificatie wordt genegeerd wanneer met SSO ingelogd wordt.
    d. Een inlogmonitor logt ongeautoriseerde inlogpogingen. Deze gegevens zijn in te zien op aanvraag.

e. Het dataverkeer tussen TriasWeb en de gebruiker kan middels IP-filtering beperkt worden. Verkeer naar TriasWeb dat niet van geaccepteerde IP-adressen komt wordt geblokkeerd.
f. TriasWeb wordt regelmatig, in ieder geval jaarlijks, door een onafhankelijke organisatie getest op integriteit, vertrouwelijkheid en beschikbaarheid.
g. TriasWeb maakt gebruik van beveiligde verbindingen op basis van certificaten.

4. Data
    a. Het is niet mogelijk om de databaseservers te benaderen van buiten het interne netwerk in het serverpark.
    b. De communicatie tussen TriasWeb en de databases wordt gereguleerd door een firewall.
    c. Productiedatabases worden dubbel uitgevoerd en zijn versleuteld.
    d. Er worden dagelijkse en maandelijkse back-ups gemaakt van de databases. Dagelijkse back-ups worden 14 dagen bewaard. Maandelijkse back-ups worden drie maanden bewaard.
    e. Gegevens van verschillende klanten zijn deels fysiek van elkaar gescheiden (ze zijn opgeslagen in verschillende databases) en deels logisch (ze worden uniek geïdentificeerd per klant). De logische scheiding wordt softwarematig afgedwongen.
5. Continuïteit
    a. Alle gegevens in TriasWeb kunnen door beheerders zelf geëxporteerd worden naar een standaard uitwisselingsformaat.
    b. Calamiteiten
    **c.** In geval van informatie-incidenten, calamiteiten of datalekken kan 24 uur per dag en 7 dagen per week contact opgenomen worden met een Information Security Officer van Triaspect. Het nummer van de ISO is te vinden op de website of via het emailadres iso@triaspect.nl. In de autoresponder vindt u het telefoonnummer dat u kunt bellen.

**Bijlage 3: Contactinformatie mbt. Inbreuken/Verzoeken van Betrokkenen**

Contactinformatie van Verwerkingsverantwoordelijke zal via e-mail door Triaspect opgevraagd worden.

Contactinformatie van Verwerker:

| | |
|---|---|
| Privacy | Triaspect |
| Functie | FG |
| Naam | Kim Alders |
| Mailadres | iso@triaspect.nl |
| Datalekken | iso@triaspect.nl |
| Telefoon | |

**In geval van informatie-incidenten, calamiteiten of datalekken kan 24 uur per dag en 7 dagen per week contact opgenomen worden met een Information Security Officer van Triaspect. Het nummer van de ISO is te vinden op de website of via het emailadres iso@triaspect.nl. In de autoresponder vindt u het telefoonnummer dat u kunt bellen.**

**Certificeringsdocumentatie**

Ons NEN-7510-certificaat , de verklaring van toepasselijkheid (losse bijlage) en het scopedocument vindt u hier: https://docs.triasweb.nl/TRIAS/certificaat-scope-en-vvt-voor-nen-7510. Bij deze vo behoren de versies die geldig zijn op de datum van deze vo.