Model Verwerkersovereenkomst Brancheorganisaties Zorg

verenigd in

12 december 2017

VERWERKERSOVEREENKOMST

DE ONDERGETEKENDEN:

1. gevestigd te en ingeschreven in het register van de Kamer van Koophandel onder nummer , hierna: "**Verwerkingsverantwoordelijke**" en

2. **AFAS Software BV**, gevestigd aan te **Leusden** en ingeschreven in het register van de Kamer van Koophandel onder nummer **31046821**, 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 in Bijlage 1 omschreven overeenkomsten.
(b) De diensten 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 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 Overeenkomst(en) van gelijke strekking tussen Partijen vervangt.

VERKLAREN TE ZIJN OVEREENGEKOMEN ALS VOLGT:

Artikel 1. Definities

1.1. 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)	Overeenkomst(en)	de in Bijlage 1 vermelde 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.

1.2. Voornoemde 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 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.
1.4. Eventuele afwijkingen op de tekst zijn alleen geldig voor zover deze zijn gespecificeerd in bijlage 4. Het bepaalde in bijlage 4 prevaleert op het overigens bepaalde in deze verwerkersovereenkomst.

Artikel 2. Onderwerp van deze Verwerkersovereenkomst

2.1. Deze Verwerkersovereenkomst heeft betrekking op de verwerking van Persoonsgegevens door Verwerker in opdracht van de Verwerkingsverantwoordelijke in het kader van de uitvoering van de Overeenkomst(en).
2.2. Partijen sluiten de Overeenkomst(en) om de expertise die Verwerker heeft als het gaat om het verwerken en beveiligen van Persoonsgegevens te gebruiken voor de uit de Overeenkomst(en) voortvloeiende en in deze Verwerkersovereenkomst nader beschreven doeleinden. Verwerker staat er voor in dat hij hiertoe gekwalificeerd is.
2.3. Deze Verwerkersovereenkomst maakt onverbrekelijk deel uit van de Overeenkomst(en). Voor zover het bepaalde in de Verwerkersovereenkomst strijdig is met het bepaalde in de Overeenkomst(en), 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 Overeenkomst (binnen de kader als gespecificeerd in Bijlage 1); of
   b.) Verwerkingsverantwoordelijke daartoe nadere schriftelijke instructies heeft gegeven;
3.2. In het kader van het bepaalde in het eerste lid van artikel 3 onder a) zal Verwerker uitsluitend de in Bijlage 1 gespecificeerde Persoonsgegevens verwerken in het kader van de in die bijlage beschreven aard en doeleinden van de verwerking.
3.3. 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.
3.4. 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.

3.5. 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 en Verwerkingsverantwoordelijke op eerste verzoek een kopie van dat register verstrekken.

3.6. Indien de dienstverlening door Verwerker de verwerking van gezondheidsgegevens of andere bijzondere Persoonsgegevens impliceert, garandeert Verwerker dat hij niet in strijd met gezondheidswetgeving zal handelen.

3.7. 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”).

3.8. Verwerker waarborgt dat betrokken Medewerkers een geheimhoudingsovereenkomst hebben getekend en geeft Verwerkingsverantwoordelijke op verzoek inzage in deze geheimhoudingsovereenkomst.

Artikel 4. Beveiliging Persoonsgegevens en controle

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 overeenstemmen met 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 van de gegevens te garanderen. In deze beveiligings-maatregelen zijn de mogelijk in de Overeenkomst 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 de 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 Persoonsgegevens te garanderen;
f.) maatregelen om te waarborgen dat Persoonsgegevens logisch gescheiden worden verwerkt van de Persoonsgegevens die hij voor zichzelf of namens derde partijen verwerkt;
g.) de overige maatregelen die Partijen zijn overeengekomen zoals vastgelegd in Bijlage 2.

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 het eerste lid van dit artikel 4 genoemde maatregelen uiteen zijn gezet.

4.3. Verwerker voldoet aantoonbaar aan de veiligheidseisen voor netwerkverbindingen zoals beschreven in NEN7512.

4.4. Verwerker voldoet aantoonbaar aan de eisen ten aanzien van logging zoals beschreven in NEN7513.

4.5. Verwerker voldoet aantoonbaar aan de eisen van andere NEN-normen voor zover die voor de gezondheidszorg van toepassing zijn verklaard.

4.6. Verwerker zal op eerste verzoek van Verwerkingsverantwoordelijke een door een onafhankelijke en ter zake deskundige derde afgegeven geldig certificaat overleggen, indien deze daarover beschikt, waaruit volgt dat Verwerker de verplichtingen uit dit artikel naleeft.

4.7. Verwerkingsverantwoordelijke heeft het recht toe te (laten) zien op de naleving van de hiervoor onder artikel 4.1 tot en met 4.4 genoemde maatregelen. Verwerker stelt Verwerkingsverantwoordelijke, indien Verwerkingsverantwoordelijke daarom verzoekt, hiertoe in elk geval eenmaal 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, dat te (laten) controleren. Verwerker zal in alle redelijkheid haar medewerking verlenen aan een dergelijk onderzoek. 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.

4.8. 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 beveiligingsmaatregelen en over de resultaten van de monitoring in overeenstemming met dit artikel 5 rapporteren aan Verwerkingsverantwoordelijke.

5.2. Zodra zich een Incident voordoet, heeft voorgedaan of zou kunnen voordoen, is Verwerker verplicht Verwerkingsverantwoordelijke daarvan onmiddellijk in kennis te stellen en daarbij alle relevante informatie te verstrekken over:
   1) de aard van het Incident;
   2) de (mogelijk) getroffen Persoonsgegevens;
   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 zonder uitstel 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 stelt Verwerkingsverantwoordelijke in staat 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 informeren van de Autoriteit Persoonsgegevens (AP) en/of de Betrokkene zoals bepaald in artikel 5.8.

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. Verwerker zal Verwerkingsverantwoordelijke voorzien van een afschrift van dergelijke procedures indien Verwerkingsverantwoordelijke daarom verzoekt.

5.6. Meldingen die worden gedaan op grond van artikel 5.2 worden ogenblikkelijk gericht aan Verwerkingsverantwoordelijke of, indien relevant, aan een door Verwerkingsverantwoordelijke tijdens de duur van deze Verwerkersovereenkomst schriftelijk bekendgemaakte Medewerkers van Verwerkingsverantwoordelijke. Indien Verwerkingsverantwoordelijke een Functionaris voor de Gegevensbescherming (FG) heeft aangesteld, worden de meldingen gericht aan deze FG.

5.7. Het is Verwerker niet toegestaan informatie te verstrekken over Incidenten aan betrokkenen of andere derde partijen, behoudens voor zover Verwerker daartoe wettelijk verplicht is of Partijen anderszins zijn overeengekomen.

5.8. Indien en voor zover Partijen zijn overeengekomen dat Verwerker in relatie tot een Incident rechtstreeks contact onderhoudt met autoriteiten of andere derde partijen, dan houdt de Verwerker de Verwerkingsverantwoordelijke daarvan voortdurend op te hoogte.

Artikel 6. Medewerkingsverplichtingen

6.1. De AVG en overige (privacy)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 klacht of een verzoek van een Betrokkene met betrekking tot verwerking van Persoonsgegevens wordt door Verwerker zonder uitstel 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 eerste 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 privacy impact assessment).

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 voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke. Het voorgaande is niet van toepassing op de in Bijlage 1 vermelde Subverwerkers.

7.2. Voor zover Verwerkingsverantwoordelijke instemt met de inschakeling van een Subverwerker, zal Verwerker aan deze Subverwerker dezelfde of strengere 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 overeenkomst(en).

7.3. Niettegenstaande de toestemming van Verwerkingsverantwoordelijke voor het inschakelen van een Subverwerker die in opdracht van de Verwerker (gedeeltelijk) gegevens verwerkt, blijft Verwerker volledig aansprakelijk jegens Verwerkingsverantwoordelijke voor de gevolgen van het uitbesteden van werkzaamheden aan een Subverwerker De toestemming van Verwerkingsverantwoordelijke voor het uitbesteden van werkzaamheden aan een Subverwerker laat onverlet dat voor de inzet van Subverwerkers in een land buiten de Europese Economische Ruimte toestemming vereist is in overeenstemming met artikel 3.7 van deze Verwerkersovereenkomst.

Artikel 8. Aansprakelijkheid

8.1. Partijen zijn ieder verantwoordelijk en aansprakelijk voor hun eigen handelen.

8.2. Enige beperking van de aansprakelijkheid in de Overeenkomst is *mutatis mutandis* ook van toepassing op deze Verwerkersovereenkomst, met dien verstande dat:

a.) eventuele (impliciete of expliciete) uitsluitingen van aansprakelijkheid voor verlies en/of verminking van Persoonsgegevens zijn uitgesloten;

b.) eventuele (impliciete of expliciete) uitsluitingen van aansprakelijkheid voor boetes die door de Autoriteit Persoonsgegevens of een andere toezichthouder worden opgelegd die rechtstreeks verband houden met een toerekenbare tekortkoming van Verwerker, of een aan Verwerker toerekenbaar gedraging of nalaten, zijn uitgesloten.

8.3. Verwerker vrijwaart Verwerkingsverantwoordelijke en stelt de Verwerkingsverantwoordelijke schadeloos voor alle claims, acties, aanspraken van derden, alsmede boetes van de Autoriteit Persoonsgegevens, die rechtstreeks voortvloeien uit 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 van toepassing zijnde wetgeving op het gebied van verwerking van Persoonsgegevens.

8.4. Voor zover Partijen hoofdelijk aansprakelijk zijn jegens derden, waaronder begrepen de betrokkene, of gezamenlijk een boete opgelegd krijgen door de Autoriteit Persoonsgegevens, zijn zij jegens elkaar, ieder voor het gedeelte van de schuld dat hem in hun onderlinge verhouding aangaat, verplicht overeenkomstig het bepaalde in Boek 6, Titel 1, Afdeling 2 van het Burgerlijk Wetboek in de schuld en kosten bij te dragen, tenzij de AVG anders bepaalt in welk geval de AVG voorgaat.

8.5. Voor zover in de Overeenkomst geen beperking van aansprakelijkheid voor Verwerkingsverantwoordelijke is opgenomen, geldt de in lid 2 opgenomen beperking voor Verwerker eveneens voor de Verwerkingsverantwoordelijke.

8.6. Iedere beperking van aansprakelijkheid komt voorts voor de betreffende Partij te vervallen in geval van opzet of grove schuld aan de zijde van de betreffende Partij.

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

Artikel 9. Kosten

9.1. De kosten voor de verwerking van gegevens die inherent zijn aan de normale uitvoering van de Overeenkomst, worden geacht besloten te liggen in de op grond van de Overeenkomst reeds verschuldigde vergoedingen.

9.2. Enige ondersteuning of enige andere aanvullende dienstverlening die Verwerker op grond van deze Verwerkersovereenkomst dient te verlenen, of die wordt verzocht door Verwerkingsverantwoordelijke, inclusief alle verzoeken tot aanvullende informatie, zullen in rekening worden gebracht bij Verwerkingsverantwoordelijke overeenkomstig de in Bijlage 3. gespecificeerde tarieven.

9.3. De voorgaande bepaling is niet van toepassing indien de werkzaamheden verband houden met een tekortkoming van Verwerker onder deze Verwerkersovereenkomst. De werkzaamheden zullen in dat geval kosteloos worden verricht (onverminderd het recht van Verwerkingsverantwoordelijke de daadwerkelijk geleden schade op Verwerker te verhalen).

Artikel 10. Duur en beëindiging

10.1. Deze Verwerkersovereenkomst gaat in op de datum van ondertekening en de duur van deze Verwerkersovereenkomst is gelijk aan de duur van de in Bijlage 1 genoemde Overeenkomst(en), inclusief eventuele verlengingen daarvan.

10.2. De Verwerkersovereenkomst maakt na ondertekening ervan door beide Partijen integraal en onlosmakelijk deel uit van de Overeenkomst(en). Beëindiging van de Overeenkomst(en), 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.

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

10.4. Ieder der Partijen is gerechtigd, onverminderd hetgeen daartoe bepaald is in de Overeenkomst, de uitvoering van deze Verwerkersovereenkomst en de daarmee samenhangende Overeenkomst 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 [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 surséance van betaling aanvraagt.

10.5. 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. Deze aanvullende afspraken kunnen onder meer bestaan uit:
   a.) het maken van afspraken over het periodiek terug of aan een derde partij leveren van de door Verwerker verwerkte gegevens; en/of
   b.) het met een derde partij sluiten van een overeenkomst die ertoe strekt dat de betreffende derde partij zich hoofdelijk verbindt tot of borg staat voor de nakoming van de Overeenkomst; en/of
   c.) het met een derde partij sluiten van een (tri-partite) overeenkomst die ertoe strekt dat de betreffende derde partij (voortdurend) over alle benodigde gegevens komt te beschikken om in voorkomend geval (een deel van) de op grond van de Overeenkomst te verrichten prestaties – al dan niet op basis van een nieuwe overeenkomst – in plaats van of parallel aan Verwerker te kunnen (gaan) verrichten.

10.6. Verwerker heeft een exit-plan voor het nakomen van alle verplichtingen uit deze Verwerkersovereenkomst, ingeval de Overeenkomst of de Verwerkersovereenkomst (tussentijds) beëindigd wordt. Verwerker geeft op eerste verzoek van Verwerkingsverantwoordelijke afschrift van dit plan.

10.7. Verwerkingsverantwoordelijke is gerechtigd deze Verwerkersovereenkomst en de Overeenkomst 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.

10.8. Verwerker dient Verwerkingsverantwoordelijke voorafgaand en tijdig te informeren over een voorgenomen overname of eigendomsoverdracht.

10.9. 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.

Artikel 11. Bewaartermijnen, teruggave en vernietiging van Persoonsgegevens

11.1. 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.

11.2. 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 onherroepelijk (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, onherroepelijke 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 12. Intellectuele eigendomsrechten

12.1. 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 13. Slotbepalingen

13.1. De overwegingen maken onderdeel uit van deze Verwerkersovereenkomst.

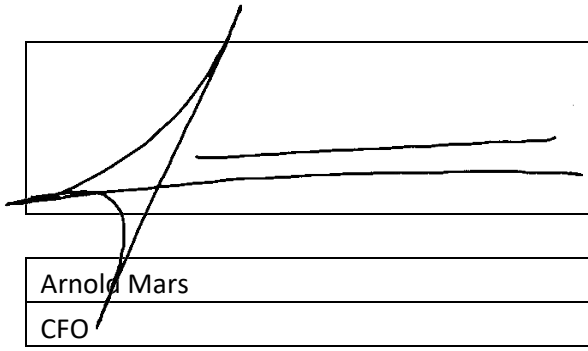
13.2. In geval van nietigheid c.q. vernietigbaarheid van een of meer bepalingen uit deze Verwerkersovereenkomst, blijven de overige bepalingen onverkort van kracht.

13.3. In alle gevallen waarin deze Verwerkersovereenkomst niet voorziet beslissen Partijen in onderling overleg.

13.4. Op deze Verwerkersovereenkomst is Nederlands recht van toepassing.

13.5. Partijen zullen zich inspannen conflicten in onderling overleg op te lossen. Hierbij is inbegrepen de mogelijkheid het geschil te beëindigen door een in onderling overleg vast te stellen mediation of arbitrage.

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

Verwerkersverantwoordelijke:	Verwerker:
	AFAS Software
	
	Arnold Mars
	CFO

Plaats: _____

Datum:_____

Plaats: Leusden

Datum: 11-7-2019

Bijlage 1: Overeenkomsten, omschrijving Persoonsgegevens, aard verwerkingen, etc.

Deze Verwerkersovereenkomst is een bijlage bij de volgende Overeenkomsten en heeft betrekking op de volgende verwerkingen van Persoonsgegevens.

Ingangs datum contract	Korte omschrijving diensten	Aard van de verwerking	Soort Persoonsgegevens	Categorieën van betrokkenen	Doeleinden van de verwerking	Goedgekeurde subverwerkers	Afspraken bewaartermijnen
	Beschikbaar stellen van een omgeving t.b.v. personneels- en/of salarisadministratie (hosting)	Verwerking Personeels- en/of salarisadministratie (HRM/Payroll)	BSN-nummer, NAW gegevens, financiële gegevens, functioneringsinformatie, personeelsdossier, Contactgegevens, administratieve gegevens	Personeelsleden, vrijwilligers, personeel niet in loondienst en andere relaties	Voldoen aan de wettelijke verplichting tot het voeren van een personeels- en/of salarisadministratie voor interne bedrijfsvoerings-doeleinden.	Leaseweb	Zie bijlage 4
	Beschikbaar stellen van een omgeving t.b.v. financiële administratie (hosting)	Verwerking financiële-administratie (Financieel)	NAW gegevens en financiële gegevens	Debiteuren en Crediteuren (ook mogelijk personen)	Voldoen aan de wettelijke verplichting tot het voeren van een financiële administratie voor interne bedrijfsvoerings-doeleinden.	Leaseweb	Zie bijlage 4

Bijlage 2 Omschrijving nadere beveiligingsmaatregelen

0. Naam

Wat is de naam van de dienst	AFAS Profit

1. Algemeen

1.1 Eis	Wij ontvangen graag een technisch plaatje van de inrichting, inclusief de informatiestromen.
Voldoet	Ja / ~~Nee~~
Toelichting	**Zie https://klant.afas.nl/afas-online**

1.2 Eis	Hebt u een escrow overeenkomst? Een escrow-overeenkomst is een overeenkomst tussen de maker van software, zijn klanten en een escrow-agent. De overeenkomst garandeert dat de klant in bepaalde gevallen kan beschikken over de laatste broncode van het softwarepakket waarvoor de overeenkomst gesloten is.
Voldoet	~~Ja /~~ Nee
Toelichting	**AFAS Software is een standaard applicatie waarbij het bezit van broncode voor een individuele klant geen toegevoegde waarde heeft. Indien gewenst kan wel een Escrow overeenkomst worden afgesloten.**

1.3 Eis	De dienst moet geïmplementeerd zijn op een (server) infrastructuur welke zich bevindt op Europees grondgebied (EER) en valt onder Europese wetgeving.
Voldoet	Ja / ~~Nee~~
Toelichting	Zie https://klant.afas.nl/sla/verwerkersovereenkomst 'Subverwerkers'

1.4 Eis	De dienst voldoet aantoonbaar aan de NEN 75xx norm voor Informatiebeveiliging in de Zorg (i.g.v. patiëntgegevens), de NEN ISO 27001 Code voor Informatiebeveiliging (i.g.v. persoons- of bedrijfsgegevens) of de ISAE3402 (internationale standaard voor zekerheid bij outsourcing). De hierbij behorende rapportage, Verklaring van Toepasselijkheid (VvT), dient op verzoek van de opdrachtgever kosteloos ter beschikking te worden gesteld.
Voldoet	Ja / ~~Nee~~
Toelichting	Zie https://klant.afas.nl/certificeringen

1.5 Eis	De (server)infrastructuur waarop de dienst is geïmplementeerd moet gehuisvest zijn in een fysieke omgeving (computerruimte) die aantoonbaar adequaat is ingericht en beveiligd volgens de genoemde NEN en ISO norm.
Voldoet	Ja / ~~Nee~~
Toelichting	Zie https://www.leaseweb.com/nl/certificeringen

1.6 Eis	De dienst wordt minimaal 1 keer per jaar onderworpen aan een uitgebreide beveiligingstest die wordt uitgevoerd door een gerenommeerde externe partij.
Voldoet	Ja / ~~Nee~~
Toelichting	Ja, dit is onderdeel van de ISO27001 certificering

1.7 Eis	Leverancier verschaft inzicht in de aard en omvang van de uitgevoerde beveiligingstest(en) alsmede de resultaten ervan.
Voldoet	Ja / ~~Nee~~
Toelichting	Zie https://klant.afas.nl/certificering/attack-penetration-test

1.8 Eis	Leverancier hanteert strikte procedures en werkinstructies voor beheer, onderhoud en ontwikkeling
Voldoet	Ja / ~~Nee~~
Toelichting	Zie https://klant.afas.nl/certificering/iso-9001

1.9 Eis	Leverancier heeft een proces voor vulnerability- & patch management
Voldoet	Ja / ~~Nee~~
Toelichting	

1.10 Eis	Opdrachtgever heeft het recht om eens per jaar het gebruik van de interne werkprocessen en procedures te toetsen middels een audit. Leverancier werkt hier kosteloos aan mee.
Voldoet	Ja / Nee
Toelichting	**Opdrachtgever heeft wel het recht, het zal niet per definitie kosteloos zijn.**

1.11 Eis	Leverancier stelt zich op de hoogte van de datalekprocedure van opdrachtgever en is bereid om die procedure zo goed mogelijk te laten aansluiten op die van opdrachtgever.
Voldoet	Ja / ~~Nee~~
Toelichting	Zie https://klant.afas.nl/sla/verwerkersovereenkomst Meldplicht datalekken

2. Infrastructuur

2.1 Eis	Alle verbindingen naar betrokken partijen (ziekenhuis, leverancier, derde partij, browser en client) over het internet zijn versleuteld. De versleuteling voldoet volledig aan de actuele richtlijn van het NCSC opgesteld in document "ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)".
Voldoet	Ja / ~~Nee~~
Toelichting	Zie https://klant.afas.nl/afas-online/architectuur

2.2 Eis	TLS certificaten dienen te zijn uitgegeven en ondertekend door een erkende CA.
Voldoet	Ja / ~~Nee~~
Toelichting	Zie https://klant.afas.nl/afas-online/architectuur

2.3 Eis	Mailservers ondersteunen STARTTLS en DANE zoals beschreven in de "Factsheet Beveilig verbindingen van mailservers" van het NCSC
Voldoet	Ja / ~~Nee~~
Toelichting	**Beperkt. Een deel van deze oplossing is mogelijk niet met de mailservers van AFAS Online te realiseren, maar prima bij gebruik van de eigen mailservers van de klant en die mogen ook gebruikt worden.**

2.4 Eis	Mailservers maken gebruik van e-mailauthenticatie zoals beschreven in de "Factsheet Bescherm domeinnamen tegen Phising" van het NCSC
Voldoet	Ja / ~~Nee~~
Toelichting	**Dit ligt voor een groot deel bij de klant zelf cq eigen mailservers. Zie ook vorig antwoord**

2.5 Eis	De webapplicatie voldoet volledig aan de actuele richtlijn van het NCSC, opgesteld in document "ICT-Beveiligingsrichtlijnen voor Webapplicaties" . Hierin worden zaken benoemd zoals meerdere lagen voor een applicatie (web- en database server), segmentering en versleuteling.
Voldoet	Ja / ~~Nee~~
Toelichting	**Wellicht niet 'volledig' maar voor de meeste zaken voldoen we hieraan.**

2.6 Eis	Er wordt gebruik gemaakt van IPS/IDS op de Next Generation Firewall, Web Application Firewall en/of Application Delivery Controller.
Voldoet	Ja / ~~Nee~~
Toelichting	

2.7 Eis	Er wordt gebruik gemaakt van on-demand malware scanners op alle besturingssystemen.
Voldoet	Ja / ~~Nee~~
Toelichting	

2.8 Eis	Er wordt gebruikt gemaakt van correlatie en signalering door middel van een overkoepelend managementsysteem (Security Monitoring en Incident Response)
Voldoet	Ja / ~~Nee~~
Toelichting	

2.9 Eis	Er wordt dagelijks gecontroleerd op nieuwe kwetsbaarheden en waar

	nodig worden beveiligingsupdates direct doorgevoerd.
Voldoet	Ja / ~~Nee~~
Toelichting	

2.10 Eis	Alle componenten van de infrastructuur worden structureel voorzien van nieuwe versies van besturings- en toepassings- en andere relevante programmatuur.
Voldoet	Ja / ~~Nee~~
Toelichting	

3. Toegang

3.1 Eis	Voor toegangsbeheer naar de applicatie wordt de NEN75xx norm gehanteerd.
Voldoet	~~Ja~~ / Nee
Toelichting	**AFAS hanteert de ISO27001 norm**

3.2 Eis	Aanvullend op NEN75xx, worden er complexiteitseisen aan het wachtwoord gesteld, die zorgen voor een sterk wachtwoord.
Voldoet	Ja / ~~Nee~~
Toelichting	
3.3 Eis	Indien er (bijzondere)persoonsgegevens worden verwerkt, is toegang tot de applicatie alleen mogelijk met Multifactor Authenticatie (MFA), bijvoorbeeldDIGID, token of sms)
Voldoet	Ja / ~~Nee~~
Toelichting	Zie

3.4 Eis	Het wachtwoord kan niet lokaal worden onthouden
Voldoet	Ja / ~~Nee~~
Toelichting	

4. Browser/Client

4.1 Eis	Browser: de webapplicatie werkt met de laatste versie van populaire browsers, zoals Internet Explorer, Chrome en Firefox.
Voldoet	Ja / ~~Nee~~
Toelichting	Zie https://www.afas.nl/systeemeisen

4.2 Eis	Browser: er zijn geen plug-ins nodig om de webapplicatie met de browser te starten.
Voldoet	Ja / ~~Nee~~
Toelichting	

4.3 Eis	Browser: De webapplicatie voldoet aan de cookiewet.
Voldoet	Ja / ~~Nee~~
Toelichting	

4.4 Eis	Browser: er worden geen cookies aangeboden die privacy gevoelige informatie opvragen van het apparaat.
Voldoet	Ja / ~~Nee~~
Toelichting	

4.5 Eis	Client: De applicatie werkt op de laatste versie van Windows, iOS en Android.
Voldoet	Ja / ~~Nee~~
Toelichting	

4.6 Eis	Client: De applicatie maakt gebruik van een sterke versleuteling bij het opslaan van het gegevens op het apparaat.
Voldoet	Ja / Nee
Toelichting	**Welke gegevens?**

4.7 Eis	Client: Het wachtwoord kan niet offline worden gekraakt.
Voldoet	Ja / Nee
Toelichting	**n.v.t.**

5. Database

5.1 Eis	Indien de dienst gebruikt maakt van één database voor het bedienen van meerdere klanten, dient er een strikte scheiding aanwezig te zijn tussen de gegevens van de verschillende klanten.
Voldoet	Ja / Nee
Toelichting	**n.v.t. Geen database voor verschillende klanten**

5.2 Eis	Alle acties en transacties op de database dienen gelogd te worden. De log moet o.m. inzichtelijk kunnen maken wie, wanneer welke tabellen in de database heeft geraadpleegd of gemuteerd. De log moet minimaal één jaar worden bewaard.
Voldoet	Ja / ~~Nee~~
Toelichting	

5.3 Eis	Het is voor een eindgebruiker niet mogelijk om de database rechtstreeks te openen.
Voldoet	Ja / ~~Nee~~
Toelichting	

5.4 Eis	Binnen de database dient een adequate rechtenstructuur te zijn geïmplementeerd, gebaseerd op rollen.
Voldoet	Ja / Nee
Toelichting	**Niet binnen de database, maar wel binnen de applicatie**

5.5 Eis	Er moet een back-up beleid aanwezig zijn die voldoet aan de NEN7510 en ISO 27001 norm. Hierin staat o.m. beschreven met welke frequentie back-ups worden gemaakt, welke bewaartermijnen worden gehanteerd, hoe restores worden uitgevoerd en wat het maximale dataverlies is. Tevens dienen restores periodiek aantoonbaar te worden getest.
Voldoet	Ja / ~~Nee~~
Toelichting	Zie https://klant.afas.nl/sla/afas-online

5.6 Eis	De data dient te zijn versleuteld met sterke versleutelingmethodieken volgens de laatste stand der techniek.
Voldoet	~~Ja~~ / Nee
Toelichting	Op dit moment is de fysieke database niet versleuteld. De vraag zou ook niet alleen moeten zijn 'of' de database is versleuteld, maar meer hoe het sleutelbeleid er dan uitziet. Als de database namelijk versleuteld is met een 'algemeen' beschikbare sleutel, welke toegevoegde waarde zou dit dan hebben. AFAS is momentele in onderzoek om de databases te versleutelen i.c.m. een HSM voor het sleutelbeheer.

Bijlage 3: Specificatie tarieven

Niet van toepassing

Bijlage 4 - Aanpassingen t.o.v. standaard tekst

Bij voorkeur wordt de gehele tekst van de modelovereenkomst gehandhaafd, uitgezonderd Bijlagen 1, 2 en 3 die per overeenkomst specifiek moeten worden ingevuld.

Mochten er toch additionele wijzigingen in de tekst nodig zijn (na onderhandelingen tussen Opdrachtgever en Opdrachtnemer) dan kunnen de aanpassingen in deze Bijlage 4 beschreven worden onder opgave van

- Artikelnummer,
- Betreffende tekst uit de standaard die vervalt
- Nieuwe vervangende tekst
- Reden van wijziging (bijv. n.v.t., eis niet acceptabel voor Opdrachtnemer, onderhandeld, etc.)

Art.	Tekst die vervalt	Vervangende tekst	Reden
4.2, 4.3, 4.4 en 4.5	De tekst in uit deze artikelen vervalt volledig, wordt vervangen:	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 het eerste lid van dit artikel 4 genoemde maatregelen uiteen zijn gezet. 4.3. Verwerker voldoet aantoonbaar aan de veiligheidseisen voor netwerkverbindingen zoals beschreven in NEN7512 voor zover de in de norm opgenomen eisen relevant zijn voor de Verwerkingen zoals beschreven in Bijlage 1 en door Verwerker als passend worden beoordeeld. 4.4. Verwerker voldoet aantoonbaar aan de eisen ten aanzien van logging zoals beschreven in NEN7513 voor zover de in de norm opgenomen eisen relevant zijn voor de Verwerkingen zoals beschreven in Bijlage 1 en door Verwerker als passend worden beoordeeld. 4.5. Verwerker voldoet aantoonbaar aan de eisen van andere NEN-normen voor zover die voor de gezondheidszorg van toepassing zijn verklaard en voor zover de in de norm opgenomen eisen relevant zijn voor de Verwerkingen zoals beschreven in Bijlage 1 en door Verwerker als passend worden beoordeeld.	

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 voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke. Het voorgaande is niet van toepassing op de in Bijlage 1 vermelde Subverwerkers	Verwerkings-verantwoordelijke geeft Verwerker toestemming om bij de verwerking van persoonsgegevens op grond van deze verwerkersovereenkomst gebruik te maken met subverwerkers met inachtname van het bepaalde in artikel 7.2 en 7.3. Verwerkings-verantwoordelijke heeft het recht bezwaar te maken tegen enige door Verwerker ingeschakelde Subverwerkers. Verwerker zal Verwerkings-verantwoordelijke tijdig informeren over het voornemen wijzigingen aan te brengen in de in bijlage 1 genoemde subverwerkers. Verwerkings-verantwoordelijke geeft met ondertekening van deze verwerkersovereenkomst aan geen bezwaar te hebben tegen de subverwerkers zoals genoemd in bijlage 1.	
8.3	Artikeltekst vervalt, wordt vervangen	Verwerker vrijwaart Verwerkingsverantwoordelijke en stelt de Verwerkingsverantwoordelijke schadeloos voor alle claims, acties, aanspraken van derden, alsmede boetes van de Autoriteit Persoonsgegevens, die rechtstreeks voortvloeien uit 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 van toepassing zijnde wetgeving op het gebied van verwerking van Persoonsgegevens.	
11.1	Artikel wordt aangepast	Verwerkingsverantwoordelijke bepaalt of en zo ja hoe lang gegevens bewaard moeten blijven. In geen geval bewaart Verwerker de Persoonsgegevens langer dan de door Verantwoordelijke aangegeven termijnen, ook na beëindiging van deze Verwerkersovereenkomst.	