

Verwerkersovereenkomst Brancheorganisaties Zorg

Versie Maastricht UMC+



de
Nederlandse
ggz



Verenigd in



VERWERKERSOVEREENKOMST

DE ONDERGETEKENDEN:

1. De publiekrechtelijke rechtspersoon het academisch ziekenhuis Maastricht, tevens handelend onder de naam Maastricht UMC+, gevestigd aan de P. Debyelaan 25, 6229 HX te Maastricht en ingeschreven in het register van de Kamer van Koophandel onder nummer 14124959, in deze rechtsgeldig vertegenwoordigd door mevrouw Dr. H.J.M.M. Mertens, voorzitter Raad van Bestuur (hierna: “**Verwerkingsverantwoordelijke**”); en
2. [Naam Verwerker], gevestigd aan de [adres] te [plaats] en ingeschreven in het register van de Kamer van Koophandel onder nummer [KvK-nummer], in deze rechtsgeldig vertegenwoordigd door [titel, naam en functie] (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 [titel/kenmerk/datum] waarbij deze Verwerkersovereenkomst Bijlage [X] 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.

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

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

- 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. **<ARTIKELLID DOORHALEN WANNEER ER GEEN SPRAKE IS VAN HET VERWERKEN VAN GEZONDHEIDSGEGEVENS>** 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. Aansprakelijkheid

- 8.1. Partijen zijn ieder verantwoordelijk en aansprakelijk voor hun eigen handelen.
- 8.2. Verwerker is aansprakelijk voor alle schade die Verwerkingsverantwoordelijke lijdt als gevolg van enige tekortkoming in de nakoming van deze Verwerkersovereenkomst en/of overtreding van de AVG en of andere toepasselijke privacy wet- en regelgeving. Deze aansprakelijkheid is beperkt tot een bedrag van maximaal 1,25 miljoen Euro per gebeurtenis en 2,5 miljoen Euro per kalenderjaar. Samenhangende gebeurtenissen worden daarbij aangemerkt als één gebeurtenis.
- 8.3. De beperking van de aansprakelijkheid als hiervoor bedoeld, of enige andere (impliciete of expliciete) beperking of uitsluiting van de aansprakelijkheid, komt te vervallen indien er sprake is van;
 - a) verlies en/of verminking van Persoonsgegevens;
 - b) 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;
 - c) opzet of grove schuld aan de zijde van de schadeveroorzakende Partij; of
 - d) de schadeaansprakelijkheid op basis van wet- en regelgeving niet uitgesloten kan worden.
- 8.4. Voor zover in de Hoofdovereenkomst geen beperking van aansprakelijkheid voor Verwerkingsverantwoordelijke is opgenomen, geldt de in lid 2 opgenomen beperking voor Verwerker eveneens voor de Verwerkingsverantwoordelijke.

Artikel 9. Kosten

- 9.1. 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 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 Hoofdovereenkomst inclusief eventuele verlengingen daarvan.
- 10.2. De Verwerkersovereenkomst maakt na ondertekening ervan door beide Partijen integraal en onverbreekelijk 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.
- 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 verplichtingen 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 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 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.
- 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.
- 10.6. 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.
- 10.7. 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.

- 10.8. 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.
- 10.9. 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 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 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 12. Slotbepalingen

- 12.1. In geval van nietigheid c.q. vernietigbaarheid van een of meer bepalingen uit deze Verwerkersovereenkomst, blijven de overige bepalingen onverkort van kracht.
- 12.2. Op deze Verwerkersovereenkomst is Nederlands recht van toepassing.
- 12.3. Geschillen over of in verband met deze Verwerkersovereenkomst worden uitsluitend voorgelegd aan de daartoe in de Hoofdovereenkomst aangewezen rechtbank of arbiter(s).

Namens Maastricht UMC+

<Naam Verwerker>

< Titel, naam portefeuillehouder Raad van Bestuur >

<Voorzitter/Lid Raad van Bestuur>

< Naam vertegenwoordiger Verwerker >

<Functie>

Plaats: _____

Plaats: _____

Datum: _____

Datum: _____

Bijlage 1: Omschrijving van de verwerking

Omschrijving van activiteiten en/of diensten, omvang en algemeen doel van de verwerking (benoem het aantal Persoonsgegevens/Betrokkenen):

Noem Hoofdovereenkomst: titel / kenmerk / ingangsdatum / partijen:

Geef een omschrijving van activiteiten en/of diensten:

Wat is het algemeen doel van de verwerking:

Over hoeveel Persoonsgegevens/Betrokkenen gaat het:

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.)	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.

Subverwerkers

Subverwerker	Beschrijving dienst en Persoonsgegevens	Gegevens buiten de EER	Verwerkers-overeenkomst
Naam en adres (incl. land)	Omschrijven	Ja/Nee (indien ja, vermeld land, instrument waaronder doorgifte kan plaatsvinden (hoofdstuk 5 AVG) en aanvullende maatregelen)	Ja/Nee

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 over de volgende certificering (kopieën, VvT en scopebeschrijving zijn bijgevoegd als bijlage bij deze Verwerkersovereenkomst):

Beschikt Verwerker niet over relevante certificering of beschikt Verwerker over een certificaat afgegeven door een certificerende instelling zonder accrediteringsverklaring van de Raad voor Accreditatie dan kan Verwerker met een Third Party Memorandum (TPM)¹ aantonen dat Verwerker werkt in overeenstemming met de ISO 27001 en wanneer van toepassing de NEN 7510. Deze TPM kan Verwerker dan hier toevoegen.

N.B. In alle gevallen, zowel in het geval er een certificaat of TPM is afgegeven alsook bij het ontbreken hiervan, dient Verwerker de concrete technische en organisatorische beveiligingsmaatregelen op te nemen in onderstaande tabel.

Maatregel	Kies een v/d volgende opties: * Compliant * Niet compliant * Alternatieve maatregel	Uitleg (moet altijd worden ingevuld!)
Maatregelen voor pseudonimisering en encryptie van persoonsgegevens (<i>minimaal: codering wordt geïmplementeerd in overeenstemming met industriestandaardalgoritmen en sleutellengtes. Beveiligde protocollen voor het delen van gegevens, indien van toepassing (bijv. SSL, FTPS, TLS), worden geïmplementeerd in</i>		

¹ Dit is een verklaring van een onafhankelijke derde partij, bijvoorbeeld een accountant.

<p><i>overeenstemming met industriestandaardalgoritmen en sleutellengtes)</i></p>		
<p>Maatregelen om de voortdurende vertrouwelijkheid, integriteit, beschikbaarheid en resilience van verwerkingssystemen en -diensten te garanderen (<i>minimaal: (Role Based) Toegangs- en autorisatiecontroles, scheiding van taken en gegevens, anti-malware, firewall, redundante systemen, indien van toepassing, en het regelmatig testen en evalueren van de effectiviteit van de organisatorische en technische maatregelen</i>)</p>		
<p>Maatregelen om de beschikbaarheid van en toegang tot persoonsgegevens tijdig te kunnen herstellen in geval van een fysiek of technisch incident</p>		
<p>Maatregelen voor gebruikersidentificatie en autorisatie (<i>minimaal: tweefactorauthenticatie, persoonlijke accounts, beperkte toegang op basis van rol, sterke wachtwoorden</i>)</p>		
<p>Maatregelen ter bescherming van persoonsgegevens tijdens overdracht (<i>minimaal: Beveiligde protocollen voor het delen van gegevens, indien van toepassing (bijv. SSL, FTPS, TLS), worden geïmplementeerd in overeenstemming met industriestandaardalgoritmen en sleutellengtes</i>)</p>		

Maatregelen ter bescherming van persoonsgegevens tijdens opslag (<i>minimaal: encryptie, firewalls en antivirus- en antimalwaresoftware</i>)		
Maatregelen ter waarborging van de fysieke beveiliging van locaties waar persoonsgegevens worden verwerkt		
Maatregelen om de logging van gebeurtenissen /incidenten te garanderen		
Maatregelen voor het borgen van de logging van brondocumentatie en datamanagementsystemen (eCRF) (indien van toepassing)		
Maatregelen om de systeemconfiguratie te garanderen, inclusief de standaardconfiguratie		
Maatregelen voor het interne IT- en IT-beveiligingsbeheer en -management		
Maatregelen om dataminimalisatie te garanderen (en/of als er geen gegevens worden verzameld, bijvoorbeeld om geen verwerking op meerdere locaties te garanderen)		
Maatregelen om een beperkte gegevensretentie te garanderen		
Maatregelen om gegevensportabiliteit mogelijk te maken en verwijdering te garanderen		
Maatregelen om een beleid inzake de vertrouwelijkheid van werknemers te waarborgen		

<p><i>(minimaal: medewerkers zijn op de hoogte van en getraind op het gebied van informatiebeveiliging en privacy en hebben een geheimhoudingsverklaring getekend)</i></p>		
<p>Maatregelen om ervoor te zorgen dat de (mede) verwerkingsverantwoordelijke volledige informatie ontvangt in geval van een inbreuk in verband met persoonsgegevens (datalek) <i>(minimaal: datum/duur, oorzaak, omvang, aard van de inbreuk, mogelijke risico's en gevolgen, genomen maatregelen ter voorkoming en controle, soort persoonsgegevens)</i></p>		
<p>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</p>		

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

Een inbreuk of andere relevante zaken dienen onmiddellijk gemeld te worden bij de volgende medewerkers van verwerkingsverantwoordelijke:

Naam: dhr. ing. J. Lamers
Functie: Stafadviseur Informatieveiligheid en Datalek coördinator
Organisatie-eenheid: Servicebedrijf Medische Instrumentatie en Informatie Technologie, Privacy & Security Office
Tel.no.: 0031 43 3874001 (secretariaat MIT)
Mobiel: 0031 6 29633734
Email: privacy@mumc.nl

Naam: mw. Y. Stienen
Functie: Stafadviseur Informatieveiligheid en Datalek coördinator
Organisatie-eenheid: Servicebedrijf Medische Instrumentatie en Informatie Technologie, Privacy & Security Office
Tel.no.: 0031 43 3874004 (secretariaat MIT)
Mobiel: 0031 6 29633724
Email: privacy@mumc.nl

Contactinformatie Verwerker:

Bijlage 4: Aanpassingen t.o.v. standaard tekst <OPTIONEEL>

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

Bijlage 5: Specificatie tarieven

[Hier uitwerken of en zo ja welke tarieven in rekening mogen worden gebracht voor uit de verwerkersovereenkomst voortvloeiende werkzaamheden]

Bijlage 6: Afwijkingen van de Verwerkersovereenkomst versie Maastricht UMC+,

Afwijkingen versie Maastricht UMC+ ten opzichte van de in december 2022 gepubliceerde standaard Verwerkersovereenkomst Brancheorganisaties Zorg.

Afwijking no.	Artikel, bijlage in versie Maastricht UMC+	Aard van afwijking
1	Titel	“Versie Maastricht UMC+” toegevoegd
2	Ondergetekenden	Benoemen ondergetekende academisch ziekenhuis Maastricht.
3	Overwegingen	Overweging (g) weggehaald.
4	1.4 en bijlage 4	Toegevoegd, afwijkingen ten opzichte van versie Maastricht UMC+, reden van bijlage 4.
5	1.5 en bijlage 6	Toegevoegd, afwijkingen versie Maastricht UMC+, reden van bijlage 6.
6	2.2	Bijlagen toegevoegd
7	Artikelkeuze en lid 4.3	Optie artikel 4 zonder gezondheidsgegevens doorgehaald. Artikellid 4.3 optioneel gemaakt
8	8	Artikel 8 toegevoegd (aansprakelijkheidsbepaling)
10	10.4.b.	Woord “ernstig” verwijderd.
11	Ondertekening	Aanpassing sjabloontekst duiding verwerkingsverantwoordelijke.
12	Bijlage 2	Tabel met concrete technische en organisatorische maatregelen toegevoegd
13	Bijlage 3	Contactgegevens contactpersonen Maastricht UMC+ toegevoegd
14	Bijlage 4	Bijlage met eventuele wijzigingen t.o.v. standaardtekst toegevoegd
15	Bijlage 5	Specificatie met tarieven toegevoegd
16	Bijlage 6	Wijzigingen versie Maastricht UMC+ t.o.v. standaardtekst toegevoegd