VU medisch centrum

Team Privacybescherming en Informatiebeveiliging

Januari 2017

Model Bewerkersovereenkomst

DE ONDERGETEKENDEN:

VU medisch centrum, gevestigd aan de De Boelelaan 1117 (1081 HV) te Amsterdam en ingeschreven in het register van de Kamer van Koophandel onder nummer 64156338 (hierna "Verantwoordelijke")

en

[*Naam Bewerker*], gevestigd aan de [*straatnaam en huisnummer*] ([*postcode*]) te [*plaats*] en ingeschreven in het register van de Kamer van Koophandel onder nummer [*KvK-nummer*] (hierna "Bewerker").

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

VERKLAREN TE ZIJN OVEREENGEKOMEN ALS VOLGT:

Artikel 1. Definities

1.1 Voor zover begrippen met een hoofdletter niet afzonderlijk gedefinieerd zijn in deze bewerkersovereenkomst, gelden de definities zoals genoemd in de toepasselijke Algemene Inkoop Voorwaarden (AIV). Begrippen uit de Wet bescherming persoonsgegevens ("Wbp"), inclusief Meldplicht datalekken zoals "verwerken", "persoonsgegevens", "verantwoordelijke", "bewerker" en "datalek" hebben de betekenis die daaraan is gegeven in de Wbp.

Artikel 2. Onderwerp van deze bewerkersovereenkomst

2.1 Bewerker kan gedurende de uitvoering van hoofdovereenkomst *[naam en datum overeenkomst]* ten behoeve van VU medisch centrum persoonsgegevens verwerken. Een overzicht van de categorieën Persoonsgegevens, de doeleinden waarvoor de persoonsgegevens worden verwerkt en een omschrijving van de bewerking(en) zijn opgenomen in Annex 1 bij deze Bewerkersovereenkomst.

Artikel 3. Uitvoering verwerking

3.1 Leverancier zal optreden als bewerker en VU medisch centrum als verantwoordelijke.

3.2 Bewerker garandeert dat hij ten behoeve van VU medisch centrum uitsluitend persoonsgegevens zal verwerken op een wijze die - en voor zover dit - noodzakelijk is voor de levering van de Prestaties zoals in de hoofdovereenkomst opgenomen. Overige verwerkingen zullen uitsluitend worden uitgevoerd in expliciete opdracht van VU medisch

centrum of als daartoe een wettelijke verplichting bestaat. In geen geval zal Bewerker persoonsgegevens verwerken voor eigen doeleinden.

3.3 Bewerker zal alle redelijke instructies van VU medisch centrum in verband met de verwerking van de persoonsgegevens opvolgen. Bewerker stelt VU medisch centrum onmiddellijk op de hoogte indien naar zijn oordeel instructies in strijd zijn met de toepasselijke wetgeving met betrekking tot de verwerking van persoonsgegevens of met een tussen partijen geldende overeenkomst.

3.4 Bewerker zal de persoonsgegevens op behoorlijke en zorgvuldige wijze en in overeenstemming met de op hem als bewerker op grond van de Wet bescherming persoonsgegevens rustende verplichtingen verwerken. Bewerker zal zich tevens houden aan de bepalingen die op grond van de Wet geneeskundige behandelingsovereenkomst (Wgbo) die van toepassing zijn op VU medisch centrum. Partijen sluiten de overeenkomst om te profiteren van de expertise die Bewerker heeft als het gaat om het beveiligen en het verwerken van Persoonsgegevens voor de doeleinden die uiteengezet zijn in Annex 1 bij deze Bewerkersovereenkomst. Het is Bewerker toegestaan om naar eigen inzicht de middelen aan te wenden die hij noodzakelijk acht om die doeleinden na te streven.

3.5 Bewerker zal, tenzij hij hiervoor uitdrukkelijke voorafgaande schriftelijke toestemming heeft verkregen van VU medisch centrum en voldaan wordt aan alle wettelijke vereisten, geen persoonsgegevens doorgeven aan landen buiten de Europese Economische Ruimte ("EER") zonder een passend beschermingsniveau. Bewerker stelt de in Annex 3 genoemde medewerker van VU medisch centrum onmiddellijk op de hoogte van alle (geplande) permanente of tijdelijke doorgiftes van persoonsgegevens naar een land buiten de Europese Economische Ruimte zonder passend beschermingsniveau en zal pas uitvoering geven aan dergelijke (geplande) doorgiftes na schriftelijke toestemming van VU medisch centrum. VU medisch centrum heeft te allen tijde het recht om aanvullende voorwaarden te verbinden aan haar toestemming voor een dergelijke verwerking.

3.6 Onverminderd enige andere contractuele geheimhoudingverplichting die op Bewerker rust, garandeert Bewerker dat hij alle persoonsgegevens als strikt vertrouwelijk zal behandelen en dat hij al zijn werknemers, vertegenwoordigers en/of sub-bewerkers die betrokken zijn bij de verwerking van de Persoonsgegevens van de vertrouwelijke aard van dergelijke informatie en van de Persoonsgegevens op de hoogte zal stellen. Bewerker zal waarborgen dat dergelijke personen en partijen een adequate geheimhoudingsovereenkomst hebben getekend en dat zij zich houden aan de bepalingen van deze Bewerkersovereenkomst en zal VU medisch centrum op verzoek van kopieën van deze overeenkomsten voorzien. Het is Bewerker niet toegestaan de Persoonsgegevens aan enige derde te tonen, verstrekken of anderszins ter beschikking te stellen, tenzij dit noodzakelijk of toegestaan is ingevolge de opdracht zoals neergelegd in de in lid 1 genoemde Annex 1 of in het geval hiervoor expliciete voorafgaande schriftelijke toestemming van VU medisch centrum is verkregen.

3.7 Bewerker zal zijn volledige medewerking verlenen aan VU medisch centrum om (i) na goedkeuring van en in opdracht van VU medisch centrum betrokkenen toegang te laten krijgen tot de hun betreffende persoonsgegevens, (ii) persoonsgegevens te verwijderen of te corrigeren, (iii) aan te tonen dat persoonsgegevens verwijderd of gecorrigeerd zijn indien zij incorrect zijn (of, ingeval VU medisch centrum het er niet mee eens is dat persoonsgegevens incorrect zijn, het feit vast te leggen dat de betrokkene zijn persoonsgegevens als incorrect beschouwt) en (iv) VU medisch centrum anderszins in de gelegenheid te stellen om aan haar verplichtingen onder de Wbp of andere toepasselijke wetgeving op het gebied van verwerking van persoonsgegevens te voldoen.

3.8 Bewerker zal de persoonsgegevens betreffende VU medisch centrum strikt gescheiden opslaan en verwerken van de persoonsgegevens die zij voor zichzelf of namens derde partijen verwerkt.

Artikel 4. Beveiliging persoonsgegevens & controle

4.1 Onverminderd de beveiligingsnormen die Partijen elders zijn overeengekomen, zal Bewerker aantoonbaar conform de NEN7510:2011 norm (norm voor Informatiebeveiliging voor de zorgsector in Nederland) passende technische en organisatorische beveiligingsmaatregelen nemen, die gezien de huidige stand der techniek en de daarmee gemoeide kosten overeenstemmen met de aard van de te verwerken persoonsgegevens, ter bescherming van de persoonsgegevens tegen verlies, onbevoegde kennisname of onrechtmatige verwerking. Deze maatregelen omvatten in ieder geval:

(a) maatregelen om te waarborgen dat enkel bevoegd personeel toegang heeft tot de persoonsgegevens voor de doeleinden die zijn uiteengezet in Annex 1;

(b) maatregelen om de persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, onopzettelijk verlies of wijziging, onbevoegde of onrechtmatige opslag verwerking, toegang of openbaarmaking;

(c) 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 VU medisch centrum;

(d) de maatregelen die Partijen in Annex 2 zijn overeengekomen.

4.2 Bewerker heeft te allen tijde een passend, geschreven beveiligingsbeleid geïmplementeerd voor de verwerking van persoonsgegevens, waarin in ieder geval de in lid 1 van dit artikel 4 genoemde maatregelen uiteen zijn gezet.

4.3 VU medisch centrum heeft het recht toe te zien op de naleving van de hiervoor onder 4.1 en 4.2 genoemde maatregelen. Bewerker stelt VU medisch centrum, indien VU medisch centrum 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 VU medisch centrum daar aanleiding toe ziet naar aanleiding van (vermoeden van) informatie- of privacy-incidenten. Bewerker zal eventuele door VU medisch centrum naar aanleiding van een dergelijke controle in redelijkheid gegeven instructies tot aanpassing van het beveiligingsbeleid binnen een redelijke termijn opvolgen.

4.4 Bewerker zal in alle redelijkheid en op eigen kosten aan het onder 4.3 hiervoor bedoelde onderzoek haar medewerking verlenen.

4.5 Partijen erkennen dat beveiligingseisen voortdurend veranderen en dat een effectieve beveiliging frequente evaluatie en regelmatige verbetering van verouderde beveiligingsmaatregelen vereist. Bewerker zal daarom de maatregelen zoals geïmplementeerd op basis van dit artikel 4 voortdurend evalueren en verscherpen, aanvullen of verbeteren om te blijven voldoen aan zijn verplichtingen onder dit artikel 4.

Artikel 5. Monitoring, informatieplichten en incidentenmanagement

5.1 Bewerker zal actief monitoren op inbreuken op de beveiligingsmaatregelen en over de resultaten van de monitoring in overeenstemming met dit artikel 5 rapporteren aan VU medisch centrum binnen de daarvoor gestelde wettelijke termijnen.

5.2 Zodra zich een incident met betrekking tot de verwerking van de persoonsgegevens voordoet, heeft voorgedaan of zou kunnen voordoen met betrekking tot beveiligingsmaatregelen, is Bewerker verplicht VU medisch centrum daarvan onverwijld in kennis te stellen en daarbij alle relevante informatie te verstrekken omtrent de aard van het incident, het risico dat gegevens onrechtmatig verwerkt zijn of kunnen worden en 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 Bewerker zal VU medisch centrum te allen tijde haar medewerking verlenen en zal de instructies van VU medisch centrum opvolgen, met als doel VU medisch centrum in staat te

stellen een deugdelijk onderzoek te verrichten naar het incident, een correcte respons te formuleren en passende vervolgstappen te nemen ten aanzien van het incident.

5.4 Onder "incident" wordt in elk geval het volgende verstaan:

(a) een klacht of (informatie)verzoek van een natuurlijk persoon met betrekking tot de verwerking van persoonsgegevens door Bewerker;

(b) een onderzoek naar of beslaglegging door overheidsfunctionarissen op de persoonsgegevens of een vermoeden dat dit gaat plaatsvinden;

(c) iedere ongeautoriseerde toegang, verwerking, verwijdering, verlies of enige vorm van onrechtmatige verwerking van de persoonsgegevens;

(d) een doorbreking van de beveiliging en/of de vertrouwelijkheid, zoals uiteengezet in artikel 3 en 4 van deze bewerkersovereenkomst, die leidt tot onopzettelijke of onrechtmatige vernietiging, verlies, wijziging, onbevoegde openbaarmaking van – of toegang tot – de persoonsgegevens, of enige aanwijzing dat een dergelijke inbreuk zal plaatsvinden of heeft plaatsgevonden.

5.5 Bewerker zal te allen tijde geschreven procedures voorhanden hebben die hem in staat stellen om VU medisch centrum van een onmiddellijke reactie over een incident te voorzien, en om effectief samen te werken met VU medisch centrum om het incident af te handelen en zal VU medisch centrum voorzien van een exemplaar van dergelijke procedures indien VU medisch centrum daarom verzoekt.

5.6 Meldingen die worden gedaan op grond van dit artikel worden gericht aan de in Annex 3 opgenomen werknemer van VU medisch centrum of, indien relevant, aan een andere door VU medisch centrum tijdens de duur van deze bewerkersovereenkomst schriftelijk bekendgemaakte andere werknemer van VU medisch centrum.

5.7 VU medisch centrum zal, indien naar haar oordeel noodzakelijk, betrokkenen, toezichthouders en andere derden informeren over incidenten. Het is Bewerker niet toegestaan informatie te verstrekken over incidenten aan betrokkenen of andere derde partijen, behoudens voor zover Bewerker daartoe wettelijk verplicht is.

Artikel 6. Gebruik onderaannemers

6.1 Bewerker zal zijn activiteiten die (deels) bestaan uit het verwerken van persoonsgegevens of vereisen dat persoonsgegevens verwerkt worden niet uitbesteden aan een derde partij (subbewerker) zonder voorafgaande schriftelijke toestemming van VU medisch centrum.

6.2 Bewerker zal aan de door hem ingeschakelde subbewerker dezelfde of strengere verplichtingen opleggen als voor hemzelf uit deze bewerkersovereenkomst en de wet voortvloeien en ziet toe op de naleving daarvan door de derde.

6.3 Niettegenstaande de toestemming van VU medisch centrum voor het inschakelen van een derde partij blijft Bewerker volledig aansprakelijk jegens VU medisch centrum voor de gevolgen van het uitbesteden van werkzaamheden aan een subbewerker. De toestemming van VU medisch centrum voor het uitbesteden van werkzaamheden aan een subbewerker laat onverlet dat voor de inzet van sub-bewerkers in een land buiten de Europese Economische Ruimte zonder een passend beschermingsniveau toestemming vereist is in overeenstemming met artikel 3.5 van deze Bewerkersovereenkomst.

Artikel 7. Aansprakelijkheid

7.1 Bewerker vrijwaart VU medisch centrum en stelt VU medisch centrum schadeloos voor alle claims, acties, aanspraken van derden en voor verliezen, schade of kosten die VU medisch centrum maakt of lijdt en die rechtstreeks of indirect voortvloeien uit of tot stand komen in verband met een tekortkoming door Bewerker of subbewerker in de nakoming van zijn verplichtingen onder deze bewerkersovereenkomst en/of enige schending door Bewerker of subbewerker van de van toepassing zijnde wetgeving op het gebied van verwerking van

persoonsgegevens in verband met de in de hoofdovereenkomst opgenomen werkzaamheden, waaronder in elk geval de Wbp.

Artikel 8. Duur en beëindiging

8.1 Deze bewerkersovereenkomst wordt ingegaan op [*datum*] en de duur van deze bewerkersovereenkomst is [*jaren/maanden*].

8.2 Verplichtingen welke naar hun aard bestemd zijn om ook na beëindiging van deze bewerkersovereenkomst voort te duren, blijven na beëindiging van de bewerkersovereenkomst gelden. Tot deze bepalingen behoren onder meer die welke voortvloeien uit de bepalingen betreffende geheimhouding, aansprakelijkheid en toepasselijk recht.

Artikel 9. Bewaartermijnen, teruggave en vernietiging van Persoonsgegevens

9.1 Bewerker bewaart de persoonsgegevens niet langer dan strikt noodzakelijk en in geen geval langer dan tot het einde van deze bewerkersovereenkomst of, indien tussen partijen een bewaartermijn is overeengekomen, niet langer dan deze termijn.

9.2 Bij beëindiging van de bewerkersovereenkomst, of indien van toepassing aan het einde van de overeengekomen bewaartermijnen, of op schriftelijk verzoek van VU medisch centrum zal Bewerker de persoonsgegevens vernietigen of teruggeven aan VU medisch centrum, naar keuze van VU medisch centrum. Op verzoek van VU medisch centrum verstrekt Bewerker bewijs van het feit dat de gegevens vernietigd of verwijderd zijn. Indien teruggave, vernietiging of verwijdering niet mogelijk zijn, stelt Bewerker VU medisch centrum daarvan onmiddellijk op de hoogte. In dat geval garandeert Bewerker dat hij de persoonsgegevens vertrouwelijk zal behandelen en niet langer zal verwerken.

9.3 Bij het einde van de bewerkersovereenkomst zal Bewerker alle derden die betrokken zijn bij het verwerken van persoonsgegevens op de hoogte stellen van de beëindiging van de bewerkersovereenkomst en zal waarborgen dat alle betrokken derden de persoonsgegevens vernietigen of aan VU medisch centrum overdragen, naar keuze van VU medisch centrum.

Artikel 10. Slotbepalingen

10.1 In het geval van strijdigheid tussen de bepalingen uit deze bewerkersovereenkomst en bepalingen uit de in hoofdovereenkomst, dan zullen de bepalingen van de bewerkersovereenkomst leidend zijn.

10.2 Op deze bewerkersovereenkomst zijn de bepalingen van de is Nederlands recht van toepassing. Geschillen over of in verband met deze Bewerkersovereenkomst worden uitsluitend voorgelegd aan de bevoegde rechter in Amsterdam.

VU medisch centrum	[*Invullen naam Bewerker*]
Plaats: ……	Plaats:
Datum: ……	Datum: ……

_____ _____

[*Naam vertegenwoordiger VU medisch centrum*] [*Naam vertegenwoordiger Bewerker*]
[*Functie*] [*Functie*]

ANNEX 1: Te verwerken persoonsgegevens, doeleinden en omschrijving bewerking(en)

[*Opnemen persoonsgegevens die zullen worden verwerkt de doeleinden waarvoor ze verwerkt zullen worden en omschrijving van bewerking(en)*]

ANNEX 2: Beveiligingsmaatregelen

[*Opnemen overeengekomen beveiligingsmaatregelen*]

ANNEX 3: Contactgegevens

contactgegevens medewerker VU medisch centrum waarmee contact dient te worden opgenomen in het geval van "incidenten"/datalekken