ADDENDUM LEVERANCIERSOVEREENKOMST M.B.T. GEGEVENSBESCHERMING

Tussen

Het Jan Yperman ziekenhuis vzw
met zetel te Briekestraat 12, 8900 Ieper
rechtsgeldig vertegenwoordigd door dhr. Frederik Chanterie, algemeen directeur
Hierna genoemd **'het Ziekenhuis'**

En

[Naam firma]
met zetel te [adres]
rechtsgeldig vertegenwoordigd door [naam en functie]
Hierna genoemd **'de Leverancier'**

Hierna gezamenlijk genoemd **'de Partijen'**

Overwegende dat

De Leverancier diensten verricht ten behoeve van het Ziekenhuis, zoals beschreven in de Basisovereenkomst, deze diensten met zich brengen dat persoonsgegevens worden verwerkt en de partijen met dit Addendum de afspraken wensen vast te leggen over de verwerking van persoonsgegevens in het kader van de diensten.

De Leverancier een expert is in de leveringen en/of diensten die het voorwerp zijn van de Basisovereenkomst, de Leverancier beschikt over de nodige middelen om de leveringen en/of diensten te volbrengen volgens de regels van de kunst en dit kan aantonen middels relevante en betrouwbare referenties.

wordt overeengekomen als volgt

1. BEGRIPPENKADER

1.1 Voor de toepassing van dit Addendum gelden de volgende begripsomschrijvingen:

- **Algemene Verordening Gegevensbescherming**: 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, met haar wijzigingen en Europese uitvoeringswetgeving;
- **Wetgeving Gegevensbescherming**: de Algemene Verordening Gegevensbescherming, andere Europese regelgeving waarin bepalingen met betrekking tot gegevensbescherming en privacy worden opgenomen, evenals de toepasselijke nationale wetgeving inzake gegevensbescherming en privacy in de lidstaten met haar wijzigingen en uitvoeringsbesluiten, met inbegrip van voor de sector toepasselijke goedgekeurde gedragscodes;
- **Persoonsgegevens, Verwerking, Verwerkingsverantwoordelijke, Verwerker, Betrokkene, Toestemming**: de begripsomschrijvingen zoals bepaald in de Algemene Verordening Gegevensbescherming;
- **Basisovereenkomst**: de overeenkomst tussen het Ziekenhuis en de Leverancier, waarbij deze verwerkersovereenkomst als bijlage gevoegd wordt.

1.2 De Leverancier levert leveringen en/of diensten aan het Ziekenhuis op grond van en zoals gedefinieerd in de Basisovereenkomst. Voor de verwerkingsactiviteiten zoals bepaald in **Annex 1** bij dit Addendum geldt volgende kwalificatie:

- het Ziekenhuis bepaalt het doel en – geheel of gedeeltelijk – de middelen van de verwerking en is bijgevolg verwerkingsverantwoordelijke;
- de Leverancier verricht de verwerking van persoonsgegevens ten behoeve van het Ziekenhuis en is bijgevolg verwerker.

2. TOEPASSINGSGEBIED EN VERHOUDING MET DE BASISOVEREENKOMST

2.1 Dit Addendum maakt integraal deel uit van de Basisovereenkomst gesloten tussen het Ziekenhuis en de Leverancier. De bepalingen uit dit Addendum zijn onverkort van toepassing op alle verwerkingen van persoonsgegevens die de

Leverancier verricht in het kader van de uitvoering van de verwerkingsactiviteiten bepaald in **Annex 1**.

2.2 De bepalingen uit dit Addendum(en Annexen) gaan voor op de (eventueel andersluidende) bepalingen over gegevensbescherming en -verwerking en vertrouwelijkheid van gegevens in de Basisovereenkomst en vervangen deze.

2.3 Alle kosten die de Leverancier dient te doen om te voldoen aan de vereisten zoals vermeld in dit Addendum worden geacht begrepen te zijn in de prijs die werd opgegeven in de Basisovereenkomst, behoudens andersluidende bepaling in de Basisovereenkomst.

3. VERWERKING CONFORM DE REGELGEVING EN DE SCHRIFTELIJKE INSTRUCTIES VAN HET ZIEKENHUIS

3.1 Bij de verwerking van persoonsgegevens handelen de Partijen in overeenstemming met de Wetgeving Gegevensbescherming.

3.2 De Leverancier verwerkt de persoonsgegevens uitsluitend op basis van de schriftelijke instructies van het Ziekenhuis, eenzijdig bepaald door het Ziekenhuis en zoals opgenomen in **Annexen 1 en 2** bij deze Bijlage. Indien de schriftelijke instructies niet duidelijk zijn, meldt de Leverancier dit schriftelijk aan het Ziekenhuis waarop in onderling overleg de instructies worden verduidelijkt.

Behoudens andersluidende bepalingen in deze Bijlage, zal de Leverancier de persoonsgegevens niet voor eigen doeleinden of die van derden verwerken, noch de persoonsgegevens aan derden verstrekken, noch deze doorsturen naar een land gelegen buiten de Europese Unie zonder daartoe een schriftelijke instructie te hebben ontvangen van het Ziekenhuis. Een verwerking conform de instructies van het Ziekenhuis kan ook betekenen dat de verwerking (onmiddellijk) moet worden stopgezet.

Indien Europese of nationale regelgeving de Leverancier tot een bepaalde verwerking verplicht, stelt de Leverancier het Ziekenhuis voorafgaand aan de verwerking in kennis van dat wettelijk voorschrift, tenzij die regelgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

3.3 Het Ziekenhuis geeft instructies aan de Leverancier in overeenstemming met de Wetgeving Gegevensbescherming en waarborgt dat alle persoonsgegevens die aan de Leverancier worden toevertrouwd rechtmatig werden verkregen en kunnen worden verwerkt in het kader van de Basisovereenkomst.

4. PASSENDE TECHNISCHE EN ORGANISATORISCHE MAATREGELEN

4.1 De Partijen treffen passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen.

4.2 Bij het bepalen van de maatregelen wordt rekening gehouden met de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen.

De maatregelen omvatten, waar passend, onder meer het volgende:

a) Pseudonimisering en versleuteling van persoonsgegevens;
b) Het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;
c) Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;
d) Een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

Bij de beoordeling van het passend beveiligingsniveau wordt met name rekening gehouden met de verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens, hetzij per ongeluk hetzij onrechtmatig.

De Leverancier bevestigt om minimaal de technische en organisatorische maatregelen zoals beschreven in **Annex 2** te nemen, onverminderd de instructies die rechtstreeks voortvloeien uit de bepalingen van de Basisovereenkomst of dit Addendum of die redelijkerwijze vereist zijn voor de juiste uitvoering door de Leverancier van zijn verplichtingen.

4.3 De Leverancier zal zich richten naar de normen van goedgekeurde gedragscodes en certificeringsmechanismen zoals die gelden binnen de sector.

Het Ziekenhuis vereist dat bij de verwerking van persoonsgegevens te allen tijde conform de ISO/IEC 27001 en 27002 Standaarden gehandeld wordt. De Leverancier legt bij voorkeur certificatie van deze normen voor. Indien de Leverancier niet over ISO/IEC 27001 en 27002 certificatie beschikt, kan het Ziekenhuis andere certificaten aanvaarden, maar dient de Leverancier steeds minstens volgens de geest van de ISO/IEC 27001 en 27002 Standaarden te werken.

5. VERWERKING DOOR EEN 'SUBVERWERKER' OF WERKNEMER

5.1 De Leverancier waarborgt dat de bepalingen van dit Addendum worden nageleefd door zijn vertegenwoordigers, agenten, onderaannemers en werknemers. De Leverancier zal persoonsgegevens van het Ziekenhuis enkel delen met of beschikbaar maken voor de vertegenwoordigers, agenten, onderaannemers en werknemers die rechtstreeks betrokken zijn bij de uitvoering van de Basisovereenkomst op basis van het 'need-to-know'-principe.

De Leverancier waarborgt in het verlengde daarvan dat:

- de tot het verwerken van persoonsgegevens gemachtigde personen zich er contractueel toe hebben verbonden om de vertrouwelijkheid in acht te nemen dan wel door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden;
- dat er maatregelen zijn getroffen om ervoor te zorgen dat iedere natuurlijke persoon die handelt onder diens gezag en toegang heeft tot de persoonsgegevens, deze (behoudens andersluidende bepaling in dit Addendum) slechts in opdracht van het Ziekenhuis verwerkt, tenzij hij door Europese of nationale regelgeving tot verwerking is gehouden.

5.2 De Leverancier maakt bij de ondertekening van dit Addendum in **Annex 1** elk van de Subverwerkers of categorieën van Subverwerkers waarop beroep wordt gedaan kenbaar en het Ziekenhuis verleent door ondertekening hiervoor algemene toestemming.

De Leverancier zal elke nieuwe Subverwerker of nieuwe categorie van Subverwerkers aan het Ziekenhuis mededelen middels **Annex 5**.
Indien het Ziekenhuis binnen 14 dagen na ontvangst van de melding van de Leverancier enig bezwaar (op redelijke gronden) uit met betrekking tot de voorgestelde nieuwe Subverwerker, zal de Leverancier geen persoonsgegevens van het Ziekenhuis doorgeven aan de voorgestelde Subverwerker, tenzij met voorafgaande schriftelijke en expliciete toestemming van het Ziekenhuis.
In geval van overmacht of technische problemen kan de Leverancier een beroep doen op een nieuwe Subverwerker zonder voorafgaande kennisgeving aan het Ziekenhuis. Het Ziekenhuis houdt zich het recht voor om zich te allen tijde te verzetten tegen één of meerdere Subverwerkers.

5.3 Wanneer de Subverwerker zijn verplichtingen inzake gegevensbescherming niet nakomt, blijft de Leverancier volledig aansprakelijk ten aanzien van het Ziekenhuis voor het nakomen van de verplichtingen van de Subverwerker.

6. DOORGIFTEN NAAR EEN LAND BUITEN DE EUROPESE ECONOMISCHE RUIMTE

6.1 Indien persoonsgegevens worden doorgegeven naar een land of organisatie buiten de Europese Economische Ruimte, zal de Leverancier de waarborgen van hoofdstuk 5 AVG naleven en passende waarborgen voorzien. De Leverancier zal bij elke doorgifte buiten de Europese Economische Ruimte het Ziekenhuis informeren over:

- Het land van de doorgifte
- Het doorgifte-instrument
- De analyse en beoordeling betreffende de aanvullende maatregelen die moeten worden genomen om de doorgifte door te voeren (Transfer Impact Assessment (TIA)).

6.2 Wanneer de Leverancier de persoonsgegevens buiten de Europese Economische Ruimte zal (laten) verwerken kan het Ziekenhuis voornoemde analyse en beoordeling van het recht en/of de geldende praktijken van het derde land en de aanvullende maatregelen opvragen bij de Leverancier. De Leverancier bezorgt deze beoordeling (Transfer Impact Assessment) op eerste vraag van het ziekenhuis.

6.3 Indien het concrete doorgifte-instrument van art. 45 tot en met 49 AVG niet doeltreffend is en er geen aanvullende maatregelen worden genomen om het

niveau van gegevensbescherming zoals vastgelegd in de AVG te vrijwaren, is het de Leverancier niet toegelaten om de persoonsgegevens door te geven buiten de Europese Economische Ruimte, behoudens wanneer het Ziekenhuis voorafgaandelijk zijn schriftelijke toestemming hiervoor heeft verleend.

6.4 Dit artikel heeft tevens betrekking op eventuele doorgiftes die gebeuren door de Subverwerkers waarop de Leverancier beroep doet voor de verwerking van persoonsgegevens in opdracht van het Ziekenhuis.

7. VERLENEN VAN BIJSTAND BIJ DE VERPLICHTINGEN M.B.T. HET GEGEVENSBESCHERMINGSBELEID VAN HET ZIEKENHUIS

7.1 Rekening houdend met de aard van de verwerking en de hem ter beschikking staande informatie, verbindt de Leverancier zich ertoe bijstand te verlenen aan het Ziekenhuis in de verantwoordelijkheid van het Ziekenhuis om volgende verplichtingen in het kader van gegevensbescherming na te leven:

- het treffen van passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen;
- de mededeling door het Ziekenhuis van een inbreuk in verband met persoonsgegevens aan de toezichthoudende overheid;
- de mededeling door het Ziekenhuis van een inbreuk in verband met persoonsgegevens van de betrokkene aan de betrokkene;
- het uitvoeren van een gegevensbeschermingseffectbeoordeling (DPIA);
- het voorafgaand raadplegen door het Ziekenhuis van de toezichthoudende overheid indien uit de gegevensbeschermingseffectbeoordeling (DPIA) blijkt dat de verwerking een hoog risico zou opleveren indien het Ziekenhuis geen maatregelen neemt om het risico te beperken.

De tijd en middelen die de Leverancier spendeert voor het verlenen van de bijstand zijn voor eigen rekening van de Leverancier, behoudens andersluidende bepaling in de Basisovereenkomst.

In het verlengde van Artikel 7.1. , licht de Leverancier het Ziekenhuis omstandig en onmiddellijk in over een (vermoedelijke) inbreuk in verband met persoonsgegevens alsook over iedere gegevenslek (ook bij de Subverwerker) zodra de Leverancier hiervan kennis heeft genomen. De kennisgeving gebeurt op een dergelijke wijze dat het Ziekenhuis tijdig kan voldoen aan haar

wettelijke verplichtingen als verwerkingsverantwoordelijke onder de Wetgeving Gegevensbescherming. De Leverancier vrijwaart het Ziekenhuis conform Artikel 10.2.

Voor de melding gebruikt de Leverancier het meldingsformulier in **Annex 4**. De Leverancier levert tevens bijstand in het onderzoek naar en de beperking en remediëring van een inbreuk in verband met een verwerking van persoonsgegevens. Daarbij zal hij onder meer ook bijstand verlenen met het oog op het documenteren van maatregelen zoals gegevensbescherming door ontwerp en door standaardinstellingen.

7.2 De Leverancier stelt het Ziekenhuis onmiddellijk in kennis van enige gemaakte klacht, beschuldiging of aanvraag (ook indien afkomstig van een regulator) met betrekking tot de verwerking van persoonsgegevens door de Leverancier. De Leverancier biedt alle nodige medewerking en ondersteuning die het Ziekenhuis redelijkerwijze kan verwachten met betrekking tot dergelijke klacht, beschuldiging of aanvraag, onder meer door volledige informatie te verstrekken over dergelijke klacht, beschuldiging of aanvraag samen met een kopie van de persoonsgegevens betreffende de betrokkene in het bezit van de Leverancier.

8. VERLENEN VAN BIJSTAND BIJ DE VERZOEKEN VAN DE BETROKKENEN

8.1 Rekening houdend met de aard van de verwerking, verleent de Leverancier het Ziekenhuis door middel van passende technische en organisatorische maatregelen bijstand bij het vervullen van de plicht van het Ziekenhuis om verzoeken tot uitoefening van de rechten van de betrokkenen, zoals bepaald in de Wetgeving Gegevensbescherming, te beantwoorden.

Dit impliceert onder meer:

- dat de Leverancier alle door het Ziekenhuis opgevraagde persoonsgegevens bezorgt, binnen de door het Ziekenhuis verzochte (redelijke) tijdsspanne, in ieder geval met inbegrip van de volledige details en kopieën van de klacht, mededeling of aanvraag en enige persoonsgegevens in zijn bezit met betrekking tot een betrokkene;
- dat de Leverancier zulke technische en organisatorische maatregelen implementeert die het Ziekenhuis toelaten doeltreffend en tijdig te antwoorden op relevante klachten, mededelingen of aanvragen.

De tijd en middelen die de Leverancier spendeert voor het verlenen van de bijstand zijn voor eigen rekening van de Leverancier, behoudens andersluidende bepaling in de Basisovereenkomst.

8.2 In het verlengde van Artikel 7.1., verbindt de Leverancier zich ertoe het Ziekenhuis onverwijld in te lichten indien hij van een betrokkene (of derde handelend voor rekening van een betrokkene) een van de volgende verzoeken krijgt:

- een aanvraag tot inzage tot de persoonsgegevens die van de betrokkene worden verwerkt;
- een aanvraag tot rectificatie van onjuiste persoonsgegevens;
- een aanvraag tot wissing van persoonsgegevens;
- een aanvraag tot beperking van de verwerking van persoonsgegevens;
- een aanvraag tot het verkrijgen van een draagbare kopie van de persoonsgegevens, of tot overdracht van een kopie aan een derde;
- een bezwaar tegen enige verwerking van persoonsgegevens; of
- elke andere aanvraag, klacht of mededeling met betrekking tot de verplichtingen van het Ziekenhuis onder de Wetgeving Gegevensbescherming.

De Leverancier beantwoordt de verzoeken en aanvragen van de betrokkenen niet zelf, behoudens eventuele andersluidende schriftelijke afspraken tussen het Ziekenhuis en de Leverancier.

9. RECHT OP CONTROLE DOOR HET ZIEKENHUIS

9.1 Het Ziekenhuis heeft steeds het recht om de naleving door de Leverancier van dit Addendum te controleren. De Leverancier stelt het Ziekenhuis alle informatie ter beschikking die nodig is om de nakoming van de verplichtingen in het kader van de Wetgeving Gegevensbescherming aan te tonen. De Leverancier maakt audits, waaronder inspecties, door het Ziekenhuis of een door het Ziekenhuis gemachtigde controleur, mogelijk en draagt er aan bij. De Leverancier verleent volledige medewerking met betrekking tot een dergelijke audit en levert, op vraag van het Ziekenhuis, het bewijs van de naleving van zijn verplichtingen onder deze Bijlage.

9.2 De Leverancier stelt het Ziekenhuis binnen redelijke termijn in kennis indien naar zijn mening een instructie een inbreuk oplevert op de Wetgeving Gegevensbescherming.

10. AANSPRAKELIJKHEID

10.1 Partijen zijn ieder verantwoordelijk en aansprakelijk voor hun eigen handelen. De in dit artikel geregelde aansprakelijkheid heeft uitsluitend betrekking op de aansprakelijkheid ten gevolge van een inbreuk op de Wetgeving Gegevensbescherming en op dit Addendum.

10.2 De Leverancier vergoedt en vrijwaart het Ziekenhuis voor alle claims, acties, aanspraken van derden en voor alle schade en verliezen (waaronder ook boetes van de Gegevensbeschermingsautoriteit) die rechtstreeks of onrechtstreeks voortvloeien uit een verwerking van persoonsgegevens wanneer bij de verwerking niet is voldaan aan de specifiek tot de verwerkers gerichte verplichtingen van de Wetgeving Gegevensbescherming of wanneer buiten dan wel in strijd met de rechtmatige instructies van het Ziekenhuis is gehandeld.

10.3 De Partijen dragen zorg voor een afdoende dekking van hun aansprakelijkheid.

11. EINDE VAN DE OVEREENKOMST

11.1 Indien de Leverancier de verplichtingen uit dit Addendum niet correct vervult en nalaat passende maatregelen te treffen binnen een termijn van maximaal twee maanden, kan het Ziekenhuis – onverminderd andere beëindigingsgronden zoals voorzien in de Basisovereenkomst – de Basisovereenkomst na voormelde termijn van twee maanden onmiddellijk verbreken en/of de verwerkingsopdracht stopzetten.

11.2 Deze overeenkomst vormt een geheel met de Basisovereenkomst en volgt dan ook het lot van de Basisovereenkomst. Ingeval de Basisovereenkomst een einde neemt, blijven de bepalingen van dit Addendum evenwel gelden voor zover nodig voor de afwikkeling van de verplichtingen conform de Wetgeving Gegevensbescherming.

11.3 Onmiddellijk bij (eender welke) beëindiging of verstrijken van de Basisovereenkomst, dan wel na afloop van de bewaartermijn, zal de Leverancier – naar keuze van het Ziekenhuis – de persoonsgegevens terugbezorgen aan het Ziekenhuis en/of de persoonsgegevens volledig en

onherroepelijk wissen, en bestaande kopieën verwijderen. In het geval het Ziekenhuis kiest voor het verwijderen van de persoonsgegevens, zal de Leverancier op schriftelijk verzoek van het Ziekenhuis aantonen dat de verwijdering daadwerkelijk gebeurd is.
De Leverancier kan van het eerste lid afwijken indien de opslag van de persoonsgegevens door Europese of nationale wetgeving verplicht is en de Leverancier het Ziekenhuis over deze verplichting in kennis heeft gesteld.

12. SLOTBEPALINGEN

12.1 In geval van nietigheid of vernietigbaarheid van een of meer bepalingen van deze Bijlage, blijven de overige bepalingen onverkort van kracht.

12.2 Dit Addendum wordt beheerst door het Belgisch recht. Geschillen worden voorgelegd aan de rechtbanken/hoven in het gerechtelijk arrondissement Ieper, die exclusieve territoriale bevoegdheid hebben.

Aldus overeengekomen en opgemaakt te [gemeente] op [datum].

Frederik Chanterie Algemeen directeur	Maarten Crappé Directeur administratie en financiën
Dr. Hans Feys Hoofdarts	[Naam] Medisch diensthoofd

VZW Jan Yperman Ziekenhuis

[Naam] [Functie]	[Naam] [Functie]

Leverancier

Annexen

- Annex 1: De verwerkingsopdracht en -instructies zoals bepaald door het Ziekenhuis
- Annex 2: Overige instructies voor de verwerking van persoonsgegevens en minimale veiligheidsmaatregelen
- Annex 3: Verbintenissen in het kader van confidentialiteit
- Annex 4: Modelformulier voor melding van gegevenslekken
- Annex 5: Modelformulier voor aanpassingen aan Annex I na afsluiten verwerkingsovereenkomst

ANNEX 1

DE VERWERKINGSOPDRACHT EN -INSTRUCTIES ZOALS BEPAALD DOOR HET ZIEKENHUIS

Inleidende opmerking

In deze Annex worden de specifieke verwerkingen door de Leverancier beschreven waartoe het Ziekenhuis opdracht geeft op het ogenblik van het sluiten van de Basisovereenkomst dan wel bij ondertekening van de Bijlage.

I. Het doel van de verwerking van persoonsgegevens

De verwerking van persoonsgegevens door de Leverancier gebeurt in het kader van de uitvoering van de Basisovereenkomst.

Beschrijving van de leveringen/diensten onder de Basisovereenkomst en van de aard en het doel van de verwerking van persoonsgegevens in het kader van de leveringen/diensten:

[Aan te vullen door de Leverancier: beschrijving van de diensten onder de Basisovereenkomst en van de aard en het doel van de verwerking van persoonsgegevens in het kader van de diensten].

II. De categorieën van persoonsgegevens die het Ziekenhuis laat verwerken door de Leverancier (aanduiden wat van toepassing is en zo nodig aanvullen):

- contactgegevens
- financiële gegevens
- factuurgegevens
- loongegevens
- gegevens over gezondheid
- marketing gegevens
- gegevens over het gebruik door het Ziekenhuis van de diensten en bijhorende producten van de Leverancier
- andere (te specificeren):

  ……

III. De categorieën van betrokkenen van wie de persoonsgegevens verwerkt worden (aanduiden wat van toepassing is en zo nodig aanvullen):

- **patiënten van het Ziekenhuis**
- vertrouwenspersonen, vertegenwoordigers en contactpersonen van de patiënten van het Ziekenhuis
- zorgverleners van de patiënten van het Ziekenhuis
- personeelsleden van het Ziekenhuis
- andere (te specificeren):
  ……

IV. De verwerking van de persoonsgegevens (aanduiden wat van toepassing is en zo nodig aanvullen):

Het Ziekenhuis geeft hierbij de volgende instructies tot verwerking van de persoonsgegevens (onverminderd de instructies die rechtstreeks voortvloeien uit de bepalingen van de Basisovereenkomst of dit Addendum of die redelijkerwijze vereist zijn voor de juiste uitvoering door de Leverancier van zijn verplichtingen):

- <u>Persoonsgegevens raadplegen</u>
  Het gaat om diensten van de Leverancier waarbij de persoonsgegevens van het Ziekenhuis bekeken kunnen worden door medewerkers of Onderaannemers van de Leverancier, waaronder maar niet beperkt tot, servicedesk Diensten, (remote) monitoring Diensten, system management Diensten, technisch applicatie management, vulnerability scanning Diensten, rapporting Diensten in governance en software asset management Diensten, het leveren van support (helpdesk, remote monitoring, etc.).

- <u>Persoonsgegevens opslaan</u>
  Het gaat om diensten van de Leverancier waarbij de persoonsgegevens van het Ziekenhuis opgeslagen worden in een door de Leverancier geleverd opslagsysteem zoals onder meer maar niet beperkt tot cloud storage Diensten, cloud back-up Diensten, file Diensten, directory Diensten, managed file transfer, mail & calendaring and logfile processing.

- <u>Persoonsgegevens doorzenden</u>
  Het betreft diensten van de Leverancier waarbij persoonsgegevens van het Ziekenhuis verzonden worden van, naar of tussen applicaties op een door de Leverancier beheerd platform zoals onder meer maar niet beperkt tot LAN Diensten, Wide Area Network Diensten, data center interconnectiviteitsdiensten, Loadbalancing, SAN switch interconnects en

Diensten die geleverd worden over de Voice over Internet Protocol (VoIP).

- Persoonsgegevens bijwerken of wijzigen
  Het betreft diensten van de Leverancier waarbij persoonsgegevens van het Ziekenhuis aangepast kunnen worden zowel op manuele, als op geautomatiseerde wijze zoals bij een geautomatiseerde job flow die ondersteund wordt door een job scheduling system.

- Software testen
  Het gaat om diensten van de Leverancier waarbij databanken van het Ziekenhuis die persoonsgegevens bevatten (persoonsgegevens die niet geanonimiseerd zijn), worden gebruikt buiten de productie omgeving (in test, acceptatie,…) als onderdeel van het testproces van de Ziekenhuis software applicatie.

- Andere: ……..

De persoonsgegevens worden door de Leverancier in geen enkele omstandigheid en onder geen beding gebruikt voor andere doelen dan deze omschreven in het Addendum en deze Annex. Dit verbod geldt ook voor louter intern (her)gebruik door de Leverancier. Hiervan kan enkel afgeweken worden mits voorafgaand akkoord van het Ziekenhuis gevoegd als annex bij de verwerkingsovereenkomst.

V. De bewaartermijnen van de (verschillende categorieën) persoonsgegevens:
De Leverancier bewaart de verwerkte persoonsgegevens op adequaat beveiligde wijze gedurende de periode die nodig is voor het uitvoeren van de schriftelijke instructies van het Ziekenhuis en volgens de bepalingen zoals overeengekomen in de Basisovereenkomst.

In geval het gaat om persoonsgegevens die deel uitmaken van het patiëntendossier geldt voor het Ziekenhuis steeds een minimum bewaartermijn van 30 jaar.

VI. Lijst van Subverwerkers:

Naam subverwerker	Contact DPO	Plaats van verwerking	Aard van de verwerking

VII. Lijst van doorgifte/ transfers naar derde landen:

Gegevensexporteur	Gegevensimporteur	Land waar persoonsgegevens verwerkt worden	Doorgifte-instrument (SCC, BCR, …) en aanvullende maatregelen (indien noodzakelijk) (*)

(*) indien het Ziekenhuis gegevensexporteur is en er een beroep wordt gedaan op de European Standard Contrual Clauses (ESCC's) van de Europese Commissie, worden deze ESCC's toegevoegd als Annex 5 bij de verwerkersovereenkomst.

VIII. De Data Protection Officer of andere verantwoordelijke contactpersonen voor gegevensbescherming en -verwerking (vul aan):

Voor het Ziekenhuis

Naam: Dhr. Niels Vermeersch

Contactgegevens: dpo@yperman.net

Voor de Leverancier

Naam: [Naam]

Contactgegevens: [e-mail].

ANNEX 2

OVERIGE INSTRUCTIES VOOR DE VERWERKING VAN PERSOONSGEGEVENS EN MINIMALE VEILIGHEIDSMAATREGELEN

Het Ziekenhuis vereist dat bij de verwerking van persoonsgegevens te allen tijde conform de ISO/IEC 27001 en 27002 Standaarden gehandeld wordt. De Leverancier legt bij voorkeur certificatie voor deze normen voor. Indien de Leverancier niet over ISO/IEC 27001 en 27002 certificatie beschikt, kan het Ziekenhuis andere certificaten aanvaarden, maar dient de Leverancier steeds minstens volgens de geest van de ISO/IEC 27001 en 27002 Standaarden te werken.

De Leverancier bevestigt daarnaast om minimaal de hierna volgende technische en organisatorische maatregelen te nemen, onverminderd de instructies die rechtstreeks voortvloeien uit de bepalingen van de Basisovereenkomst of dit Addendum of die redelijkerwijze vereist zijn voor de juiste uitvoering door de Leverancier van zijn verplichtingen.

Indien de Leverancier samenwerkt met Subverwerkers, garandeert de Leverancier dat elk van de Subverwerkers werkt conform dezelfde standaarden en voldoet aan dezelfde minimumvoorwaarden.

De Leverancier bevestigt kennis te hebben genomen van de “Gedragscode informatieveiligheid voor leveranciers” en de “IT-vereisten voor PC’s, Serversoftware, medische toestellen en randapparatuur” zoals beschikbaar op de website van het Ziekenhuis.

Het Ziekenhuis kan – als onderdeel van haar informatieveiligheidsbeleid – aan de Leverancier vragen om een Leveranciersbeoordeling informatieveiligheid in te vullen.

MINIMALE MAATREGELEN VOOR DE LEVERANCIER EN HUN SUBVERWERKERS:

1. PERSOONSGEGEVENS RAADPLEGEN BIJ HET ZIEKENHUIS

Voor de verwerkingen waarbij persoonsgegevens het Ziekenhuis niet verlaten gelden cumulatief de volgende minimum maatregelen:

1.1. De persoonsgegevens kunnen enkel door het eigen personeel van de

Leverancier worden geraadpleegd en dit in zoverre strikt noodzakelijk voor het uitvoeren van de opdracht zoals omschreven in de Basisovereenkomst.

1.2. De Leverancier bezorgt op eenvoudige vraag van het Ziekenhuis een actuele lijst van de personen die voor de uitoefening van hun opdracht noodzakelijk toegang nodig hebben tot de systemen. Hierin wordt tevens de reden van de aanvraag van toegangsrechten gemotiveerd. Wijzigingen in deze lijst worden door de Leverancier onmiddellijk gecommuniceerd aan het Ziekenhuis.

1.3. Elk van de personen die toegang krijgt wordt door de Leverancier onderworpen aan de vertrouwelijkheids- en discretieplicht zoals opgesteld door het Ziekenhuis (zie **Annex 3**).

1.4. Elk van de personen die toegang krijgt tot gevoelige gegevens bij het Ziekenhuis werd door de Leverancier voldoende opgeleid en geïnformeerd over verplichtingen en verantwoordelijkheden bij het (potentieel) raadplegen van persoonsgegevens. Het Ziekenhuis kan bijkomend eisen dat een opleiding zoals ter beschikking gesteld door het Ziekenhuis gevolgd wordt.

2. PERSOONSGEGEVENS OPSLAAN BUITEN HET ZIEKENHUIS

Voor verwerkingen waarbij persoonsgegevens het Ziekenhuis verlaten en door de Leverancier (of zijn Subverwerker) worden bewaard, gelden - bijkomend aan de bovenstaande verplichtingen - cumulatief ook de volgende verplichtingen:

2.1. Door dit Addendum af te sluiten, verklaart de Leverancier over de volgende documenten te beschikken.

2.1.1. Een geïmplementeerd Informatieveiligheidsplan (Information Security Management System) samen met de bevestiging dat de policy door de hoogste hiërarchie en diverse verantwoordelijken werd goedgekeurd.

2.1.2. Een geïmplementeerd Back-up and Disaster Recovery Plan dat minstens specifieert:

- welke back-up mechanismes worden gebruikt en of deze afdoende zijn;

- welke recovery testen worden gebruikt en of de rapportering hiervan beschikbaar is.

2.1.3. Een geïmplementeerd Identity and Access management (IAM) policy die ten minste de volgende principes ondersteunt:
- duidelijk gedefinieerde, rolgebaseerde toegangsrechten;
- intrekken van toegang bij einde samenwerking;
- strong Authentication;
- full logging van IAM en data access.

2.1.4. Een geïmplementeerd Incident Management Procedure. Deze beschrijft minstens hoe gevolgen van incidenten voor de data van het Ziekenhuis beperkt worden, welke de te nemen stappen zijn bij ontdekking van een veiligheidsincident en welke personen verantwoordelijk zijn om het incident aan te pakken en zo een gezonde toestand te herstellen.

2.2. De Leverancier bevestigt te voldoen aan de volgende technische en organisatorische vereisten:

2.2.1. De gegevens verkregen van of via het Ziekenhuis mogen de grenzen van de Europese Economische Ruimte niet verlaten. Indien zij deze grenzen toch verlaten, dient de Leverancier de nodige garanties voor te leggen die bewijzen dat de doorgifte voldoet aan Hoofdstuk V van de Algemene Verordening Gegevensbescherming (Doorgifte van persoonsgegevens aan derde landen of internationale organisaties).

2.2.2. De netwerken waarover gegevens worden verstuurd (vast of draadloos, van, naar of tussen applicaties, of via een door de Leverancier beheerd platform zoals onder meer maar niet beperkt tot LAN-diensten, WAN-diensten, data center interconnectiviteitsdiensten, loadbalancing, SAN switch interconnects en diensten die geleverd worden over de VoIP) beveiligd te hebben volgens de regels van de kunst en de geldende standaarden en voor de verzending van gevoelige gegevens aangepaste technieken te gebruiken.

2.2.3. De hardware (inclusief VM) uitgerust te hebben met afdoende toezichtmechanismes en beveiligingssystemen om data lekken te voorkomen en te analyseren.

2.2.4. De gebruikte informaticasystemen overeenkomstig hun classificatie te hebben geplaatst in geïdentificeerde en beschermde lokalen waartoe de toegang beperkt is.

2.2.5. Alle server stations te hebben uitgerust met preventie en detectie mechanismen, alsook middelen om virussen en andere malware in te dijken en dienen de server stations een hardening process te hebben ondergaan.

2.2.6. Alle server stations te hebben uitgerust met een patch management proces (geïmplementeerd en gedocumenteerd).

2.2.7. Voor alle server stations patches te testen in een acceptance omgeving vooraleer deze uit te rollen.

2.2.8. De systemen minimum 1x per jaar aan een penetration test en/of ethical hacking te onderwerpen.

2.3. De Leverancier garandeert de implementatie van deze maatregelen te kunnen staven door middel van (externe) rapportering, opgemaakt met een minimum van 1x per 3 jaar en dit volgens een nauwkeurig omschreven stramien. Bij het afsluiten van de Overeenkomst kan het Ziekenhuis de laatste (externe) rapportering of een document dat aangeeft door wie, wanneer en volgens welke basis de rapportering werd opgemaakt, opvragen bij de Leverancier.

2.4. De Leverancier kan nooit overgaan tot aanpassing van de persoonsgegevens van het Ziekenhuis - hetzij op manuele dan wel op geautomatiseerde wijze - buiten voor deze gevallen waarvoor expliciete toestemming bestaat van het Ziekenhuis

2.5. De Leverancier garandeert dat bij (eender welke) beëindiging of verstrijken van de Basisovereenkomst, dan wel na afloop van de bewaartermijnen zoals voorzien in Artikel V. van **Annex I**, op vraag en naar keuze van het Ziekenhuis, alle data veilig teruggegeven (ineen voor het Ziekenhuis

leesbaar formaat) en bij de Leverancier vernietigd worden en dit voor alle media die gebruikt worden voor gegevensopslag.

ANNEX 3

VERBINTENISSEN IN HET KADER VAN CONFIDENTIALITEIT

De Leverancier en haar aangestelden zullen zich tijdens hun aanwezigheid bij Opdrachtgever steeds volledig schikken naar alle binnen Opdrachtgever geldende reglementen en voorschriften, inzonderheid naar deze die betrekking hebben op veiligheid, gezondheid en hygiëne.

Zij verbinden er zich toe om zowel tijdens hun werkzaamheid bij Opdrachtgever, als na de beëindiging hiervan, gelijk welke hem/haar ter kennis gekomen informatie die een vertrouwelijk karakter heeft of kan hebben en rechtstreeks of onrechtstreeks verband houdt met de activiteiten van of binnen Opdrachtgever (zoals alle informatie over patiënten, gegevens i.v.m. personeelsleden en personeelsaangelegenheden, verslagen, bedrijfsinformatie in de breedste zin, gegevens van medisch-technische, technische, financiële of commerciële aard …) als geheime informatie te behandelen.

Hieronder valt tevens alle vertrouwelijke informatie die meegedeeld wordt door of betrekking heeft op personen of instellingen waarmee zij tijdens hun aanwezigheid bij Opdrachtgever op welke wijze ook in contact zijn gekomen.

Indien in het kader van de opdracht toegang verleend wordt tot elektronische systemen van het Ziekenhuis, in bijzonder het systeem voor het beheer van het elektronisch patiëntendossier, zal de Leverancier of zijn/haar aangestelde zich steeds volledig schikken naar alle binnen Opdrachtgever geldende reglementen, voorschriften en procedures betreffende het gebruik van deze systemen.

Dit houdt o.a. in dat

- Om toegang te nemen tot het systeem uitsluitend persoonlijke logingegevens kunnen worden gebruikt, zoals toegekend door het Ziekenhuis;
- Het persoonlijk paswoord strikt geheim moet worden gehouden;
- Het consulteren en eventueel aanpassen van (patiënt) gegevens enkel toegestaan is binnen het kader van de overeengekomen opdracht;
- De Leverancier verantwoordelijk en aansprakelijk is voor alles wat onder log-ins van zijn/haar aangestelden gebeurt;
  De Leverancier verantwoordelijk is voor het informeren van haar aangestelden dat door Opdrachtgever van alle door haar aangestelden uitgevoerde acties logs worden bewaard.

Gegevens contactpersoon van het Ziekenhuis (bereikbaar 24/7):
Dienst: DPO
E-mail: dpo@yperman.net

Datum:
Bedrijfsnaam:
Adres:
Postcode:
BTW-nummer:
Wie heeft de inbreuk geconstateerd?
Naam:
Functietitel:
Wanneer is de inbreuk geconstateerd?
Datum:
Tijd:
Omschrijf het beveiligingsincident waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan:
Wanneer heeft de inbreuk plaatsgevonden?
a. Op (datum + tijd)
b. Tussen (datum + tijd) en (datum + tijd)
c. Is nog niet vastgesteld
d. Er is sprake van een anonieme melding door een derde
Vastleggen context van de data betrokken bij de inbreuk:

Classificatie van de data:
a. Geen, de gegevens zijn niet herleidbaar tot een individu
b. Naam, adres en woonplaats gegevens
c. Telefoonnummers
d. E-mailadressen, Facebook ID's, Twitter ID's etc.
e. Gebruikersnamen, wachtwoorden of andere inloggegevens, klantnummers
f. Financiële gegevens: rekeningnummers, creditcardnummers
g. Rijksregisternummer
h. Kopieën van identiteitsbewijzen
i. Geslacht, geboortedatum, en/of leeftijd
j. Gegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid of lidmaatschap van een vakvereniging
k. Gegevens over iemands gezondheid of seksuele geaardheid
l. Strafrechtelijke persoonsgegevens of persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag
m. Gegevens over iemands financiële of economische situatie, gegevens over schulden, salaris- en betalingsgegevens
n. Afgeleide financiële data (inkomenscategorie, huizenbezit, autobezit)
o. Lifestyle kenmerken (o.a. gezinssamenstelling, woonsituatie, interesses), demografische kenmerken (leeftijd, geslacht, nationaliteit, beroep, onderwijs)
p. Data verkregen uit (openbare) sociale profielen (Facebook-, LinkedIn- en Twitteraccounts, ...)
q. Overig, namelijk:
Classificatie van de context betrokken bij de inbreuk:
Van **hoeveel** personen zijn persoonsgegevens betrokken bij de inbreuk?
a. Geen, de gegevens zijn niet herleidbaar tot een individu
b. Nog niet bepaald
c. Ten minste …… (aantal), maar niet meer dan ……..(aantal) betrokkenen
Omschrijf de groep mensen waarvan persoonsgegevens zijn betrokken bij de inbreuk:
Omstandigheden van het gegevenslek:

a. Alleen lezen (een niet geautoriseerde derde heeft (vertrouwelijke) data kunnen inzien. Verwerker heeft de data nog in zijn bezit.) - **Confidentialiteit is in gevaar**
b. Kopiëren (een niet-geautoriseerde derde heeft data kunnen kopiëren. De data is ook nog in het bezit van Verwerker.) - **Confidentialiteit is in gevaar**
c. Wijzigen (een niet-geautoriseerde derde heeft data gewijzigd, of kunnen wijzigen, in systemen van Verwerker) - **Integriteit is in gevaar**
d. Verwijderen of vernietigen (een niet-geautoriseerde derde heeft data verwijderd uit de systemen van Verwerker of data vernietigd.) - **Beschikbaarheid is in gevaar**
e. Diefstal - **Beschikbaarheid is in gevaar**
f. Nog niet gekend
Zijn de persoonsgegevens onbegrijpelijk of ontoegankelijk gemaakt voor ongeautoriseerde derden, bijvoorbeeld door encryptie en hashing?
Ja
Nee
Deels, namelijk
Zo ja, op welke manier zijn de persoonsgegevens versleuteld:
Heeft de inbreuk betrekking op personen uit andere EU-landen?
Ja
Nee
Zo ja, welke EU-landen:
Welke beveiligingsmaatregelen (technisch en organisatorisch) zijn getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?

Wie kan benaderd worden voor meer informatie over de inbreuk?
Naam contactpersoon van de Leverancier:
E-mail:
Telefoonnummer:

ANNEX 5

MODELFORMULIER VOOR AANPASSINGEN AAN ANNEX 1 NA AFSLUITEN VERWERKINGSOVEREENKOMST

Indien de Partijen bepaalde aspecten anders of specifieker wensen te regelen of bepaalde zaken wensen toe te voegen na het afsluiten van de verwerkingsovereenkomst, dienen deze door middel van dit formulier expliciet te worden overeengekomen met het Ziekenhuis.

De wijzigingen in deze Annex zijn enkel geldig en afdwingbaar indien deze Annex door beide partijen is ondertekend en gedagtekend.

Artikel	Tekst die (eventueel) vervalt	Vervangende of toegevoegde tekst	Reden

Aldus overeengekomen en opgemaakt te [gemeente] op [datum].

Frederik Chanterie Algemeen directeur	Maarten Crappé Directeur administratie en financiën
Dr. Hans Feys Hoofdarts	[Naam] Medisch diensthoofd

VZW Jan Yperman Ziekenhuis

[Naam] [Functie]	[Naam] [Functie]

Leverancier