ADDENDUM M.B.T. GEGEVENSBESCHERMING

De Leverancier,

hierna vermeldt als "de leverancier"

verricht diensten ten behoeve van het Ziekenhuis,

de VZW Onze-Lieve-Vrouw van Troost, exploitant van het A.Z. Sint-Blasius, gevestigd te 9200 Dendermonde, Kroonveldlaan 50, BTW nr. BE0411.975.133, hierbij krachtens haar statuten rechtsgeldig vertegenwoordigd door Mevr. Karen Pieters, algemeen directeur,

hierna vermeldt als "het ziekenhuis"

zoals beschreven in de Overeenkomst. Deze diensten brengen met zich mee dat persoonsgegevens worden verwerkt.

Met dit Addendum worden de afspraken vastgelegd tussen de partijen over de verwerking van persoonsgegevens in het kader van de diensten.

Indien de Partijen in onderlinge overeenstemming aanpassingen aan de tekst van dit Addendum wensen, worden die aanpassingen – in zoverre zij in overeenstemming zijn met de Wetgeving Gegevensbescherming en onder de contractuele vrijheid van de Partijen vallen – onder opgave van de reden geregistreerd in Annex 1 bij dit Addendum.

Wijzigingen bij Annex 1 zijn enkel geldig indien ze door beide partijen zijn ondertekend en gedateerd.

1. BEGRIPPENKADER

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

- **Algemene Verordening Gegevensbescherming**: de 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;

- **Overeenkomst**: de overeenkomst tussen het Ziekenhuis en de Leverancier.

1.2 De Leverancier levert diensten aan het Ziekenhuis op grond van en zoals gedefinieerd in de Overeenkomst.

Voor de verwerkingsactiviteiten zoals bepaald in **Annex 2** bij dit Addendum geldt volgende kwalificatie:

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

2. TOEPASSINGSGEBIED EN VERHOUDING MET DE OVEREENKOMST

2.1 Dit Addendum maakt integraal deel uit van de Overeenkomst 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 2.

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 Overeenkomst en vervangen deze.

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 **Annex 2** bij dit Addendum. Indien de schriftelijke instructies niet duidelijk zijn, meldt de leverancier dit schriftelijk aan het Ziekenhuis waarop in onderling overleg de instructies worden verduidelijkt.

3.3 Behoudens andersluidende bepalingen in dit Addendum 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.

3.4 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 Overeenkomst.

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.

4.3 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 zal zich richten naar de normen van goedgekeurde gedragscodes en certificeringsmechanismen zoals die gelden binnen de sector. Hij voegt een bewijs daarvan bij als Annex bij dit Addendum.

4.4 De Leverancier beschrijft in **Annex 3** de passende technische en organisatorische maatregelen die door hem worden getroffen. Hij rapporteert op eigen initiatief aan het Ziekenhuis de wijzigingen die aan de maatregelen, zoals uiteengezet in Annex 3, worden doorgevoerd en dit binnen een termijn van veertien dagen na het aanbrengen van de wijzigingen.

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 waarborgt in het verlengde daarvan dat:

- de tot het verwerken van persoonsgegevens gemachtigde personen zich ertoe 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 slechts in opdracht van het Ziekenhuis verwerkt, tenzij hij door Europese of nationale regelgeving tot verwerking is gehouden.

5.2 De Leverancier neemt geen andere verwerker in dienst ("Subverwerker") zonder de voorafgaande specifieke of algemene schriftelijke toestemming van het Ziekenhuis.

In geval van een specifieke schriftelijke toestemming bezorgt de Leverancier in **Annex 1** de volledige details van de door de subverwerker overgenomen verwerking bij dit Addendum.

In geval van een algemene schriftelijke toestemming, schakelt de Leverancier enkel een derde partij als subverwerker in voor zover hij het Ziekenhuis tijdig en in ieder geval voorafgaand over de identiteit van de subverwerker heeft ingelicht en voorzover het Ziekenhuis zich hiertegen niet heeft verzet.

5.3 Wanneer de Leverancier een beroep doet op een subverwerker, legt de Leverancier aan deze subverwerker bij overeenkomst dezelfde verplichtingen inzake gegevensbescherming op zoals die gelden tussen Verwerker en Verwerkingsverantwoordelijke. De Leverancier bezorgt op eerste verzoek aan het Ziekenhuis de overeenkomst met de subverwerker.

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

6.1 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;
- het melden van een inbreuk in verband met persoonsgegevens aan de toezichthoudende overheid;
- de mededeling van een inbreuk in verband met persoonsgegevens aan de betrokkene;
- het uitvoeren van een gegevensbeschermingseffectbeoordeling;
- het voorafgaand raadplegen van de toezichthoudende overheid indien uit de gegevensbeschermingseffectbeoordeling 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.

6.2 In het verlengde van artikel 6.1, 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 9.2.

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.

6.3 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.

7. VERLENEN VAN BIJSTAND BIJ DE VERZOEKEN VAN DE BETROKKENEN

7.1 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 betrokkene, 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.

7.2 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.

8. RECHT OP CONTROLE DOOR HET ZIEKENHUIS

8.1 Het Ziekenhuis heeft steeds het recht om de naleving door de Leverancier van het 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 dit Addendum.

8.2 De Leverancier stelt het Ziekenhuis onmiddellijk in kennis indien naar zijn mening een instructie onder artikel 8.1 inbreuk oplevert op de Wetgeving Gegevensbescherming.

9. AANSPRAKELIJKHEID

9.1 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.

9.2 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.

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

10. EINDE VAN DE OVEREENKOMST

10.1 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 Overeenkomst – de Overeenkomst na voormelde termijn van twee maanden onmiddellijk verbreken en/of de verwerkingsopdracht stopzetten.

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

10.3 Onmiddellijk bij (eender welke) beëindiging of verstrijken van de Overeenkomst, 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.

11. SLOTBEPALINGEN

11.1 In geval van nietigheid of vernietigbaarheid van een of meer bepalingen van dit Addendum, blijven de overige bepalingen onverkort van kracht.

11.2 Dit Addendum wordt beheerst door het Belgisch recht. Geschillen worden voorgelegd aan de rechtbanken/hoven van Dendermonde, die exclusieve territoriale bevoegdheid hebben.

Annexen

Annex 1: aanpassingen aan het addendum bij contractuele vrijheid van de partijen
Annex 2: de verwerkingsopdracht en -instructies zoals bepaald door het ziekenhuis
Annex 3: de informatiebeveiliging
Annex 4: modelformulier melding gegevenslekken

ANNEX 1 – AANPASSINGEN AAN HET ADDENDUM BIJ CONTRACTUELE VRIJHEID VAN DE PARTIJEN

Het Addendum bevat een standaard tekst die uitvoering geeft aan de verplichtingen uit de Wetgeving Gegevensbescherming. Bepaalde aspecten vallen (binnen bepaalde limieten) onder de contractuele vrijheid van de partijen.

Indien de Partijen bepaalde aspecten anders of specifieker wensen te regelen of bepaalde zaken wensen toe te voegen, worden zij in deze Annex expliciet bepaald.

Tot de contractuele vrijheid kunnen bijvoorbeeld behoren:

- de termijnen waarbinnen de Leverancier het Ziekenhuis moet inlichten of bijstand moet verlenen (maar in ieder geval binnen de termijn waarbinnen het Ziekenhuis zelf aan de toezichthoudende overheid of de betrokkene dient te melden);
- specificatie of met een specifieke dan wel algemene toestemming wordt gewerkt voor de subverwerker(s);
- …

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**

ANNEX 2 - DE VERWERKINGSOPDRACHT- EN INSTRUCTIES ZOALS BEPAALD DOOR HET ZIEKENHUIS

Begeleidende nota

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

Wijzigingen en/of aanvullingen van deze Annex 2 gebeuren telkens via een afzonderlijk document dat als bijlage bij deze Annex 2 wordt gevoegd (Bijlage 1 bij Annex 2; Bijlage 2 bij Annex 2, enz.), dat wordt gedateerd en waaruit de expliciete en schriftelijke instructie en/of instemming van het Ziekenhuis blijkt.

I. Het doel van de verwerking van persoonsgegevens

De verwerking van Persoonsgegevens door de Leverancier gebeurt in het kader van de uitvoering van de Overeenkomst inzake…… *[aan te vullen door leverancier]*.

Beschrijving van de diensten onder de Overeenkomst 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
- ☐ medische gegevens
- ☐ 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 aanpassen/aanvullen waar nodig) :

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

☐ Persoonsgegevens raadplegen
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

☐ Persoonsgegevens opslag
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 backup Diensten, file Diensten, directory Diensten, managed file transfer, mail & calendaring and logfile processing.

☐ Persoonsgegevens doorzenden
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.

IV. 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 voor wat de onderstaande categorieën persoonsgegevens betreft gedurende de hierna bepaalde periode **[aanvullen indien bewaartermijn kan worden uitgedrukt in maanden]** :

- voor **[categorie gegevens invullen]** gedurende **[XX maanden na/vanaf …. bv. het laatste gebruik]**
- voor **[categorie gegevens invullen]** gedurende **[XX maanden na/vanaf … bv. het laatste gebruik]**

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

Voor het Ziekenhuis
Naam: Sabine Magerman
Contactgegevens: privacy@azsintblasius.be

Voor de Leverancier
Naam:
Contactgegevens:

ANNEX 3 – DE INFORMATIEBEVEILIGING

Vragenlijst informatieveiligheid en gegevensbescherming voor de verwerker

Naam van de organisatie (derde partij)	Benaming: ..... Adres: .... Ondernemingsnummer (KBO): .....
Voornaam, Naam & email adres van de verantwoordelijke voor informatieveiligheid (CISO) (verplicht)	....
Voornaam, Naam & email adres van het aanspreekpunt voor informatieveiligheid (adjunct CISO) (optioneel)	....
Voornaam, Naam & email adres van de functionaris voor gegevensbescherming (DPO) (verplicht)	....
Voornaam, Naam & email adres van het lokale aanspreekpunt voor gegevensbescherming (adjunct DPO of vertegenwoordiger) (optioneel)	....
Voornaam, Naam & email adres van de persoon belast met het dagelijks bestuur (CEO, verplicht)	....

Vraag	*Kruis (X) het vak aan dat overeenstemt met uw antwoord*		Leg uit bij een ´neen` antwoord
1	Beschikt u over een formeel, geactualiseerd en door de verantwoordelijke voor het dagelijks bestuur goedgekeurd beleid voor informatieveiligheid?	☐ JA ☐ NEEN	
2	Heeft u een risicobeoordeling voor elk proces/project rond informatieveiligheid/gegevensbescherming die u gebruikt voor de dienstverlening?	☐ JA ☐ NEEN	
3	Binnen uw organisatie: • is er een dienst belast met de informatieveiligheid die onder de directe, functionele leiding staat van de verantwoordelijke voor het dagelijks bestuur van de organisatie?	☐ JA ☐ NEEN ☐ JA ☐ NEEN	
4	Beschikt u over een informatieveiligheidsplan goedgekeurd door de verantwoordelijke voor het dagelijks bestuur?	☐ JA ☐ NEEN	
5	Hoeveel uren werden gepresteerd door de CISO en diens team? • CISO • Team Hoeveel uren opleidingen rond informatieveiligheid hebben de DPO en diens team gevolgd? • DPO • Team	1) uren/maand 2) uren/maand 3) uren/jaar 4) uren/jaar	
6	Beschikt u over procedures voor de ontwikkeling van nieuwe systemen of belangrijke evoluties van bestaande systemen, zodat de projectverantwoordelijke rekening kan houden met de veiligheidsvereisten die in de minimale veiligheidsnormen beschreven worden?	JA ☐ NEEN ☐ N/A ☐	
7	Neemt u de gepaste maatregelen opdat de professionele, vertrouwelijke en gevoelige gegevens opgeslagen op mobiele media enkel toegankelijk zijn voor geautoriseerde personen?	☐ JA ☐ NEEN	
8	Treft u de gepaste maatregelen, in functie van het toegangsmedium, voor de informatieveiligheid van de toegang van buiten uw organisatie tot de professionele, vertrouwelijke en gevoelige gegevens?	☐ JA ☐ NEEN	

Vraag	*Kruis (X) het vak aan dat overeenstemt met uw antwoord*		Leg uit bij een ´neen` antwoord
9	Heeft u de telewerk-voorzieningen zo ingericht dat er op de telewerk-plek (thuis, in een satellietkantoor of in een andere locatie) geen informatie wordt opgeslagen op externe toestellen zonder versleuteling en dat mogelijke bedreigingen vanaf de telewerk-plek niet in de IT-infrastructuur terechtkomen?	☐ JA ☐ NEEN	
10	Sensibiliseert u jaarlijks iedere medewerker met betrekking tot de informatieveiligheid en gegevensbescherming en voert u jaarlijks een evaluatie uit rond de naleving van dit beleid in de praktijk?	☐ JA ☐ NEEN	
11	Heeft u de toegang beveiligd door een duidelijke toegangsprocedure en heeft u een (logisch of fysiek) toegangssysteem geïmplementeerd om elke ongeoorloofde toegang te voorkomen?	☐ JA ☐ NEEN	
12	Beschikt u over een classificatieschema voor persoonsgegevens waarvoor u de diensten levert en past u dit classificatieschema toe?	☐ JA ☐ NEEN	
13	Heeft u de regels verwerkt in een beleid voor informatieveiligheid die gespecifieerd zijn in een beleidslijn ‘Email, online communicatie en internet gebruik’?	☐ JA ☐ NEEN	
14	Heeft u minstens één toegangsbeheerder aangesteld wanneer u gebruik maakt van toegang op afstand tot de zorginstelling?	☐ JA ☐ NEEN	
15	Heeft u uw medewerkers aangezet tot het lezen en toepassen van extra veiligheidsmaatregelen die de zorgvoorziening oplegt (indien van toepassing)?	☐ JA ☐ NEEN	
16	Wanneer u ‘cryptografie’ wilt toepassen: • beschikt u over een formeel beleid voor het gebruik van cryptografische controles ? • beschikt u over een formeel beleid voor het gebruik, bescherming en levensduur van de cryptografische sleutels voor de ganse levenscyclus?	☐ JA ☐ NEEN ☐ JA ☐ NEEN	
17	Neemt u de nodige maatregelen om de toegang tot de gebouwen en lokalen te beperken tot de geautoriseerde personen en verricht u een controle erop zowel tijdens als buiten de werkuren?	☐ JA ☐ NEEN	
18	Neemt u de nodige maatregelingen ter voorkoming van verlies, schade, diefstal of compromitteren van middelen en onderbreking van de activiteiten?	☐ JA ☐ NEEN	
19	Bij hergebruik van de informatiedrager gebruikt u deze opnieuw in een minstens vergelijkbaar data-classificatieniveau?	☐ JA ☐ NEEN	

Vraag	*Kruis (X) het vak aan dat overeenstemt met uw antwoord*		Leg uit bij een ´neen` antwoord
20	Legt u de gepaste maatregelen voor het wissen van gegevens contractueel vast met de opdrachtgever?	☐ JA ☐ NEEN	
21	Past u de regels toe in verband met de logging van de toegang zoals vastgelegd door de opdrachtgever?	☐ JA ☐ NEEN	
22	Zijn regels vastgelegd voor het verwerven, ontwikkelen en onderhouden van systemen tussen de verschillende betrokken partijen?	☐ JA ☐ NEEN	
23	Werken alle medewerkers met de ICT middelen in het kader van de opdracht op basis van minimale autorisatie voor de uitvoering van hun taak?	☐ JA ☐ NEEN	
24	Worden de vereisten voor toegangsbeveiliging (identificatie, authenticatie, autorisatie) gedefinieerd, gedocumenteerd, gevalideerd en gecommuniceerd? Worden deze toegangen gelogd?	☐ JA ☐ NEEN ☐ JA ☐ NEEN	
25	Worden de veiligheids- en gegevensbeschermingsrisico's contractueel vastgelegd tussen u en eventuele onderaannemers?	☐ JA ☐ NEEN	
26	Gebruikt u een controlelijst zodat de projectleider er zich kan van vergewissen dat het geheel van de beleidslijnen informatieveiligheid en gegevensbescherming correct geëvalueerd en indien noodzakelijk geïmplementeerd worden tijdens de ontwikkelingsfase van het project?	☐ JA ☐ NEEN	
27	Voert u bij elke in productiestelling van een project een controle uit of de veiligheids- en gegevensbeschermingsvereisten die bij het begin van het project werden vastgelegd ook daadwerkelijk geïmplementeerd werden?	☐ JA ☐ NEEN	
28	Worden, onder de supervisie van de projectleider, de voorzieningen voor ontwikkeling, test en/of acceptatie en productie gescheiden – inclusief de bijhorende scheiding der verantwoordelijkheden in het kader van het project?	☐ JA ☐ NEEN	
29	Wordt elke toegang tot persoonlijke en vertrouwelijke gegevens gelogd in overeenstemming met een policy "logging" en de toepasselijke wetgeving en regelgeving?	☐ JA ☐ NEEN	
30	Wordt in de specificaties van een project opgenomen hoe de toegang tot en het gebruik van systemen en applicaties gelogd zal worden om bij te dragen tot de detectie van afwijkingen inzake informatieveiligheid en gegevensbescherming?	☐ JA ☐ NEEN	

Vraag	*Kruis (X) het vak aan dat overeenstemt met uw antwoord*		Leg uit bij een ´neen` antwoord
31	Beantwoordt het logbeheer minimaal aan de volgende doelstellingen? • De informatie om te kunnen bepalen wie, wanneer en op welke manier toegang heeft verkregen tot welke informatie • De identificatie van de aard van de geraadpleegde informatie • De duidelijke identificatie van de persoon	☐ JA ☐ NEEN	
32	Zijn de noodzakelijke tools ter beschikking om toe te laten de log gegevens uit te baten door de geautoriseerde personen?	☐ JA ☐ NEEN	
33	Worden de transactionele/functionele log gegevens overeenkomstig de bewaard overeenkomstig de gegevens zelf (vb 30 jaar voor medische gegevens)?	☐ JA ☐ NEEN	
34	Worden de deliverables (gegevens die verwerkt worden, de documentatie (broncode, programma's, technische documenten, …)) van het project geïntegreerd in het back-up beheersysteem?	☐ JA ☐ NEEN	
35	Worden, in de loop van de ontwikkeling van het project, de behoeften met betrekking tot continuïteit van de dienstverlening geformaliseerd, conform met uw verwachtingen?	☐ JA ☐ NEEN	
36	Wordt uw continuïteitsplan en de bijhorende procedures geactualiseerd in functie van de projectevolutie, met inbegrip van continuïteitstesten?	☐ JA ☐ NEEN	
37	Wordt er een risico analyse in het begin van het project uitgevoerd om de noodprocedures te definiëren?	☐ JA ☐ NEEN	
38	Worden, in de loop van de ontwikkeling van het project, de procedures met betrekking tot het incidentbeheer geformaliseerd en gevalideerd?	☐ JA ☐ NEEN	
39	Wordt de CISO op de hoogte gesteld van de veiligheidsincidenten en de DPO voor incidenten inzake gegevensbescherming?	☐ JA ☐ NEEN	
40	Wordt tijdens de levensloop van het project de documentatie (technisch, procedures, handleidingen, …) actueel gehouden?	☐ JA ☐ NEEN	
41	Worden alle middelen inclusief aangekochte of ontwikkelde systemen toegevoegd aan de inventaris van de operationele middelen?	☐ JA ☐ NEEN	
42	Wordt de gepaste medewerking verleend aan audits uitgevoerd onder de vorm van het ter beschikking stellen van personeel, documentatie, logbeheer en andere informatie die redelijkerwijze beschikbaar is?	☐ JA ☐ NEEN	
43	Worden vereisten rond informatieveiligheid en gegevensbescherming gedocumenteerd om risico's te reduceren mbt toegang informatiemiddelen?	☐ JA ☐ NEEN	
45	Worden alle relevante vereisten rond informatieveiligheid en privacy opgesteld en overeengekomen tussen u en derde partijen/toeleveranciers (die informatie van	☐ JA ☐ NEEN	

Vraag	*Kruis (X) het vak aan dat overeenstemt met uw antwoord*		Leg uit bij een ´neen` antwoord
	de organisatie lezen, verwerken, stockeren, communiceren of ICT infrastructuurcomponenten en ICT diensten aanleveren)?		
46	Wordt regelmatig de dienstverlening aan u door derde partijen / toeleverancier gemonitord, geëvalueerd en geauditeerd ?	☐ JA ☐ NEEN	
47	Worden de wijzigingen in de dienstverlening aan u door de derde partij / toeleverancier beheerd, waaronder het bijhouden van bestaande beleidslijnen, procedures/maatregelen voor informatieveiligheid en gegevensbescherming ?	☐ JA ☐ NEEN	
48	Beschikt u over een beleidslijn 'Cloud computing' wanneer u een beroep doet op clouddiensten?	☐ JA ☐ NEEN	
49	Wanneer u professionele, vertrouwelijke of gevoelige gegevens wenst te verwerken in een cloud voldoet u aan de minimale contractuele waarborgen?	☐ JA ☐ NEEN	
50	Heeft u procedures voor het vastleggen en beheren van incidenten over informatieveiligheid of gegevensbescherming met de bijhorende verantwoordelijkheden en heeft u deze procedures intern bekend gemaakt?	☐ JA ☐ NEEN	
51	Heeft u een overeenkomst met alle medewerkers dat elke medewerker (zowel vast of tijdelijk, intern of extern) verplicht is melding te maken van ongeautoriseerde toegang, gebruik, verandering, openbaring, verlies of vernietiging van informatie en informatiesystemen?	☐ JA ☐ NEEN	
52	Worden de gebeurtenissen en zwakheden over informatieveiligheid of gegevensbescherming die verband houden met informatie en informatiesystemen zodanig kenbaar gemaakt aan de opdrachtgever zodat u en de opdrachtgever tijdig en adequaat corrigerende maatregelen kunnen nemen?	☐ JA ☐ NEEN	
53	Beschikt de leverancier over een procedure om zo snel als mogelijk intern incidenten inzake informatieveiligheid/gegevensbescherming te communiceren/rapporteren?	☐ JA ☐ NEEN	
54	Worden bij incidenten over informatieveiligheid of gegevensbescherming het bewijsmateriaal in overeenstemming met wettelijke en regelgevende voorschriften correct verzameld?	☐ JA ☐ NEEN	
55	Wordt elk incident over informatieveiligheid of gegevensbescherming formeel gevalideerd opdat procedures en controlemaatregelen verbeterd kunnen worden en worden de lessen die getrokken worden uit een incident gecommuniceerd naar uw directie voor validatie en goedkeuring van verdere acties?	☐ JA ☐ NEEN	

Vraag	*Kruis (X) het vak aan dat overeenstemt met uw antwoord*		Leg uit bij een ´neen` antwoord
56	Heeft u een continuïteitsplan voor alle kritieke processen en essentiële informatiesystemen?	☐ JA ☐ NEEN	
57	Is informatieveiligheid en gegevensbescherming een integraal onderdeel van uw continuïteitsbeheer?	☐ JA ☐ NEEN	
58	Heeft u een eigen continuïteitsplan? Wordt dit plan regelmatig getest en aangepast met de nodige communicatie naar uw directie voor validatie en goedkeuring?	☐ JA ☐ NEEN ☐ JA ☐ NEEN	
59	Voert u periodiek een conformiteitsaudit uit met betrekking tot de situatie rond informatieveiligheid en gegevensbescherming?	☐ JA ☐ NEEN	
60	Heeft u een formeel disciplinair proces voor werknemers die inbreuk op de informatieveiligheid of gegevensbescherming hebben gepleegd?	☐ JA ☐ NEEN	
61	Brengt u regelmatig alle informatie samen om de risico's in kaart te brengen in verband met de conformiteit met GDPR en voert u de nodige acties uit als gevolg van een hoog "residueel" risico op non-conformiteit?	☐ JA ☐ NEEN	
62	Heeft u een up-to-date centrale register van de verwerkingsverantwoordelijke of van de verwerker en heeft u een formele verantwoording voor het niet-realiseren van controlemaatregelen gericht op de naleving van de Europese verordening voor de specifieke verwerking?	☐ JA ☐ NEEN	

Datum en handtekening van de CISO of functionaris voor gegevensbeheer (DPO) van de organisatie (derde partij) (optioneel)	…… Datum Handtekening
Datum en handtekening van de persoon belast met het dagelijks bestuur van de organisatie (derde partij) **(verplicht)**	…… Datum Handtekening

******* EINDE VAN DIT DOCUMENT *******

ANNEX 4 – MODELFORMULIER MELDING GEGEVENSLEKKEN

Gegevens contactpersoon van het Ziekenhuis - az Sint-Blasius (bereikbaar 24/7):
Dienst: Directielid van wacht
Telefoonnummer 050/555.170

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. NAW-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 iemand 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 vastgesteld
c. Ten minste …… (aantal), maar niet meer dan ……..(aantal) betrokkenen
Omschrijf de groep mensen waarvan persoonsgegevens zijn betrokken bij de inbreuk:
Omstandigheden van de 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 (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 bekend
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: