VERWERKERSOVEREENKOMST INZAKE GEGEVENSBESCHERMING

Tussen ondergetekenden

Het AZ Sint-Elisabeth Zottegem vzw, waarvan de maatschappelijke zetel gevestigd is te Godveerdegemstraat 69, 9620 Zottegem, rechtsgeldig vertegenwoordigd door Frank Verbeke, algemeen directeur- dagelijks bestuurder (ondernemingsnummer 0418.558.166)

Hierna genoemd "**het Ziekenhuis**"

EN

……

[*gegevens leverancier aan te vullen*]

Hierna genoemd "**Leverancier**"

Hierna gezamenlijk genoemd de "**Partijen**"

Overwegende dat

de Leverancier diensten of goederen aanbiedt ten behoeve van het Ziekenhuis, die met zich meebrengen dat persoonsgegevens worden verwerkt en de partijen met deze verwerkersovereenkomst de afspraken wensen vast te leggen over de verwerking van die persoonsgegevens

wordt overeengekomen als volgt:

1. BEGRIPPENKADER

1.1 Voor de toepassing van deze verwerkersovereenkomst 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;

1.2 De Leverancier levert diensten of goederen aan het Ziekenhuis op grond van een samenwerkingsovereenkomst, onderhoudscontract, toegewezen aanbesteding of (diensten)order i.v.m.:
……
……
(Hierna 'Basisovereenkomst')

Voor de verwerkingsactiviteiten zoals bepaald in **Annex 1** bij deze verwerkersovereenkomst 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 of maakt deze mogelijk ten behoeve van het Ziekenhuis en is bijgevolg verwerker.

2. TOEPASSINGSGEBIED EN VERHOUDING MET DE BASISOVEREENKOMST

2.1 Deze verwerkersovereenkomst maakt integraal deel uit van de Basisovereenkomst gesloten tussen het Ziekenhuis en de Leverancier. De bepalingen uit deze verwerkersovereenkomst zijn 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 deze verwerkersovereenkomst (en Annexen) gaan voor op de (eventueel andersluidende) bepalingen over gegevensbescherming en -verwerking en vertrouwelijkheid van gegevens in de Basisovereenkomst 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 1** bij deze verwerkersovereenkomst. 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 deze verwerkersovereenkomst 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 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.

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 houdt daarvan een bewijs ter beschikking van het Ziekenhuis.

4.4 De Leverancier neemt de passende technische en organisatorische maatregelen tot naleving van de bepalingen uit **Annex 2**.

5. VERWERKING DOOR EEN "SUBVERWERKER" OF WERKNEMER

5.1 De Leverancier waarborgt dat de bepalingen van deze verwerkersovereenkomst 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 deze verwerkersovereenkomst.

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 3**.

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 de verwerkersovereenkomst 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 verwerkersovereenkomst.

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 deze verwerkersovereenkomst.

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 deze verwerkersovereenkomst 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 samenwerking na voormelde termijn van twee maanden onmiddellijk verbreken en/of de verwerkingsopdracht stopzetten.

10.2 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 deze verwerkersovereenkomst 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 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.

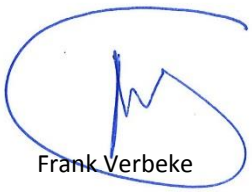
De Leverancier kan van het eerste lid afwijken indien de opslag van de persoonsgegevens door Europese of nationale wetgeving verplicht is.

11. SLOTBEPALINGEN

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

11.2 Deze verwerkersovereenkomst wordt beheerst door het Belgisch recht. Geschillen worden voorgelegd aan de rechtbanken/hoven in het gerechtelijk arrondissement Oost-Vlaanderen, afdeling Oudenaarde, die exclusieve territoriale bevoegdheid hebben.

Aldus overeengekomen en in tweevoud opgemaakt te Zottegem op 25/05/2018.



Frank Verbeke [Naam]

Het Ziekenhuis **Leverancier**

Annexen

Annex 1: de verwerkingsopdracht en -instructies zoals bepaald door het ziekenhuis
Annex 2: clausules beveiliging en informatieveiligheid
Annex 3: modelformulier melding gegevenslek door verwerker

ANNEX 1 - 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 Basisovereenkomst dan wel bij ondertekening van de verwerkersovereenkomst.

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

1. Het doel van de verwerking van persoonsgegevens

De verwerking van Persoonsgegevens door de Leverancier gebeurt in het kader van de uitvoering van de Basisovereenkomst, meer bepaald:

……
……*[aan te vullen door leverancier]*.

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

……
……
……
……
……

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

- personalia en contactgegevens van patiënten
  - financiële gegevens
  - factuurgegevens
  - loongegevens
  - gezondheid gegevens
  - marketing gegevens
- gegevens over het gebruik door het Ziekenhuis van de diensten en bijhorende producten van de Leverancier
  - identificatiegegevens werknemers en verwerker
  - logging en tijdsregistraties
- gegevens ter verificatie van toegang zoals gebruikersnaam, PC naam en IP adres
- andere (te specificeren) :

  ……
  ……
  ……

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

- patiënten
- vertrouwenspersonen, vertegenwoordigers en contactpersonen van de patiënten van het Ziekenhuis
- interne zorgverleners
- externe zorgverleners
- personeelsleden
- algemene dienstverleners in opdracht van de patiënt
- andere (te specificeren):
  ……
  ……
  ……

4. 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 Basisovereenkomst of deze verwerkersovereenkomst of die redelijkerwijs 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

- <u>Persoonsgegevens opslag</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 backup 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).

- <u>Persoonsgegevens bijwerken of wijzigen</u>
  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.

- <u>Software testen</u>

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.

- ……
- ……
- ……

[Aan te vullen]

5. 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]**

6. De Data Protection Officer of andere verantwoordelijke contactpersonen voor gegevensbescherming en -verwerking:

Voor het Ziekenhuis
Naam: Joris Sergeant
Contactgegevens: 09/364.83.30
joris.sergeant@sezz.be

Voor de Leverancier
Naam:
Contactgegevens:

ANNEX 2 - CLAUSULES BEVEILIGING EN INFORMATIEVEILIGHEID

1. INLEIDING

1.1 De leverancier verbindt zich er toe een informatieveiligheidsbeleid uit te werken volgens de principes van de ISO 27000 methodologie, meer in het bijzonder de methodologie die beschreven staat in ISO 27001:2013, de maatregelen zoals opgelijst in ISO 27002:2013 en ISO 27799:2008, zoals beschreven in de minimale normen informatieveiligheid en privacy binnen de sociale zekerheid in overeenstemming met adviezen en beslissingen van het Sectoraal comité Sociale Zekerheid en Gezondheid.

1.2 Indien de leverancier diensten aanbiedt die specifiek het verwerken van persoonsgegevens betreft, vult zij verplicht alle vragenlijsten in die betrekking hebben op de verplichtingen opgelegd aan verwerkers zoals voorzien in de Verordening (EU) 2016/679 van het Europese parlement en de raad van 27 april 2016 en de na te leven normen voorzien door de Belgische privacy toezichthouder en alle door de wet voorziene bepalingen.

1.3 Indien de leverancier diensten aanbiedt betreffende het verwerken van persoonsgegevens in de cloud dient zij alvorens zij dergelijke diensten levert een analyse te maken van de veiligheidsvoorzieningen en vult daartoe de SMALS Cloud Security Model evaluatietool in (https://www.smalsresearch.be/tools/cloud-security-model-nl/) en bezorgt daarvan het resultaat onverwijld aan het ziekenhuis.

2. AANVAARDING VAN OPDRACHT

2.1 Door aanvaarding van de opdracht en/of door verdere samenwerking gaat de leverancier akkoord met de inhoud van deze annex. Elke verkoopsvoorwaarden van de leverancier, ongeacht de benaming die eraan wordt gegeven door de leverancier, is niet van toepassing indien ze strijdig zijn met de bepalingen van deze annex.

3. RISICOBEHEER EN ORGANISATIE VAN INFORMATIEVEILIGHEID

3.1 De leverancier voert op regelmatige basis risicoanalyses uit op de geleverde producten en diensten om na te gaan in welke mate deze voldoen aan de wettelijke veiligheidsvereisten en de wettelijke verplichtingen.

3.2 De leverancier engageert zich om elk relevant risico in het product of dienstverlening binnen een zo kort mogelijke periode te melden aan het ziekenhuis. Met relevant wordt bedoeld een risico waarbij het veiligheidsniveau van de persoonsgegevens in de toepassing of dienstverlening in het gedrang komt zoals gegevenslekken, hacking, onderbreking van een systeem in productie.

3.3 De leverancier werkt volgens de ISO 27000 methodologie of gelijkaardig, en heeft een veiligheidsbeleid, veiligheidsplan en veiligheidsverantwoordelijke (veiligheidsconsulent en/of Data Protection Officer) aangesteld.

3.4 De leverancier heeft informatieveiligheid meegenomen in de overeenkomsten met personeelsleden en contractanten. Ze zijn bij gevolg op de hoogte hoe met gevoelige persoonsgegevens moet worden omgegaan.

3.5 De leverancier neemt informatieveiligheid mee in de overeenkomsten met onderaannemers. De leverancier heeft met andere woorden controle over de veiligheidsmaatregelen die de onderaannemers nemen.

3.6 De leverancier verklaart toegangscodes tot systemen die direct of indirect toegang verlenen tot informatie van het ziekenhuis of systemen die over het ziekenhuis informatie bevatten, te beheren als een goede huisvader. Dit omvat de nodige beveiligingsvereisten, ook bij beëindiging van contracten met medewerkers.

3.7 De leverancier verklaart op elk moment te kunnen nagaan wie van zijn medewerkers toegang had tot de informatie van het ziekenhuis. Om dit te realiseren, wordt gebruik gemaakt van gepersonaliseerde toegangscodes voor alle identiteiten.

3.8 De toegangscodes die worden gebruikt voor het leveren van producten en diensten zijn uniek voor het ziekenhuis en worden niet gedeeld in configuraties met andere ziekenhuizen. Voorbeelden van toegangscodes zijn deze voor het aanspreken van een databank, voor toegang tot de applicatie, voor de configuratie van geplande taken en services, voor het maken van verbindingen met externe informatiesystemen, voor de koppeling met medische apparatuur.

3.9 De leverancier verklaart toegangscodes, cryptografische sleutels en andere gevoelige informatie op een veilige manier te bewaren. Dit omvat het gebruik van beveiligde informatiecontainers die enkel toegankelijk zijn voor gemachtigde medewerkers.

4. BEVEILIGING VAN DE GEGEVENS VAN HET ZIEKENHUIS IN DE GELEVERDE TOEPASSING

4.1 De toepassingen die de leverancier levert zijn voorzien van een systeem van toegangsbeveiliging voor de eindgebruiker dat minstens voldoet aan volgende eisen:

4.1.1 De toegang is nominatief in te stellen (gebruikersnaam per gebruiker)

4.1.2 De toegangscode (wachtwoord) is vrij te kiezen door de eindgebruiker en er is een mogelijkheid om deze zelf te wijzigen;

4.1.3 De toegangscodes van de applicatie worden op een veilige manier (i.e. geëncrypteerd) uitgewisseld tussen de systeemcomponenten;

4.1.4 De toegangscodes worden in een niet leesbaar formaat bewaard in de toepassing.

4.2 Handelingen van de gebruiker in de toepassing kunnen worden opgespoord via de logging. Het omvat de logging op leesactiviteiten, wijzigingen die worden doorgevoerd, nieuwe dataelementen die worden aangemaakt of informatie die wordt verwijderd. De logging is beveiligd tegen wijzigingen.

4.3 De leverancier dupliceert nooit gegevens zonder schriftelijke toelating van het ziekenhuis. Wanneer gegevens de toepassing verlaten, bijvoorbeeld via een USB stick, door een kopij op afstand of in het kader van een klassieke uitwisseling tussen systeemcomponenten, dan neemt de leverancier veiligheidsmaatregelen om de gegevens te beveiligen. Dit is minstens encryptie van de gegevens zelf en het transportkanaal waarover de gegevens worden getransporteerd.

4.4 Wanneer de leverancier systemen voorziet of gebruikt waarop gegevens van het ziekenhuis worden bewaard (in test, demo of productie), dan zijn deze systemen beveiligd. Hieronder verstaan we dat de systemencomponenten permanent bijgewerkt zijn met de laatste bijwerkingen (bv. updates van het besturingssysteem en toepassingen), dat er beveiliging is tegen malware en dat het systeem voorzien is van een back-up.

4.5 Bij een beëindiging van de overeenkomst met de leverancier, al dan niet op een vooraf bepaald moment, behoudt het ziekenhuis het recht om de gegevens te kunnen exporteren en in een gestructureerde, gangbare en machineleesbare vorm te verkrijgen. Indien dit technisch mogelijk is, voorziet de leverancier een rechtstreeks van de ene verwerkingsverantwoordelijke naar de andere doorgezonden totale verwerking of export.

5. GEDRAGSCODE VOOR HET GEBRUIK VAN ICT-APPARATUUR EN HET NETWERK

5.1 Algemeen

5.1.1 De leverancier en de medewerkers onder zijn verantwoordelijkheid mogen de zwakheden of tekortkomingen van de beveiliging van informatiesystemen van het ziekenhuis niet aanwenden of trachten aan te wenden om toegang te krijgen tot systemen waarvoor geen gepaste vergunning werd verleend.

5.1.2 Het is verboden computerprogramma's of computermechanismen binnen het netwerk te gebruiken die de beveiliging proberen te omzeilen, of die informatie betreffende de toegangscontrole onthullen. De gekende zwakke punten of inbreuken op de beveiliging moeten onmiddellijk gemeld worden aan de dienst informatieveiligheid en/of de directeur ICT van het ziekenhuis.

5.2 ICT-Apparatuur

5.2.1 De computersystemen en andere ICT-apparatuur eigendom van het ziekenhuis, mogen enkel gebruikt worden binnen de perken van de toevertrouwde professionele opdracht. Indien praktische omstandigheden een uitzondering vereisen kunnen die enkel toegestaan worden na uitdrukkelijk overleg met en goedkeuring van de directeur ICT.

5.2.2 De leverancier en de medewerkers onder zijn verantwoordelijkheid verbinden zich ertoe de onderstaande richtlijnen te volgen. Op ICT-apparatuur van het ziekenhuis :

5.2.2.1 enkel software te gebruiken die door de onderneming wordt verstrekt en dit overeenkomstig de specifieke richtlijnen en geen andere software te installeren en/of te gebruiken;

5.2.2.2 de ingestelde veiligheidsmaatregelen (bv. de virusscanner) niet uit te schakelen;

5.2.2.3 alle bestanden verkregen via een extern netwerk of verschaft op draagbare media nodig voor de opdracht, te controleren om na te gaan of deze virusvrij zijn alvorens deze te gebruiken tijdens de opdracht;

5.2.2.4 geen gegevens van het ziekenhuis en zijn activiteiten die er mee gepaard gaan op dragers te kopiëren of aan derden mee te delen;

5.2.2.5 toegang tot beveiligde IT-ruimtes en afgeschermde netwerkapparatuur enkel onder supervisie van de dienst ICT te laten plaatsvinden;

5.2.2.6 geen foto’s of filmpjes nemen en/of publiceren waarop patiënten of ziekenhuismedewerkers herkenbaar zijn.

5.3 Het ziekenhuisnetwerk

5.3.1 Het is niet toegelaten apparatuur aan het ziekenhuisnetwerk te koppelen of wijzigingen aan te brengen aan de bestaande infrastructuur zonder de schriftelijke toestemming van de dienst ICT. Dit geldt zowel voor het bekabeld als draadloos netwerk en voor elke apparatuur al dan niet eigendom van het ziekenhuis. De leverancier dient de nodige toegangsrechten aan de directeur ICT van het ziekenhuis te verstrekken betreffende de systemen die niet vallen onder het ICT-beheer van het ziekenhuis.

5.3.2 Shares op het netwerk mogen enkel door of in opdracht van de medewerkers van de dienst ICT van het ziekenhuis aangemaakt of gewijzigd worden. Extern gebruik van het interne netwerk van het ziekenhuis is alleen toegestaan aan de daartoe geautoriseerde personen en moeten via een goedgekeurde en geregistreerde firewall lopen.

Systemen die gebruikt worden voor externe aansluiting aan het ziekenhuisnetwerk dienen voorzien te zijn van up-to-date beschermingstools conform de ISO-normering. Daarnaast dient de externe gebruiker erop toe te zien dat de systeemsoftware op zijn systeem wordt

onderhouden op een actueel patchniveau. Externe connecties worden na een door het ziekenhuis vast te stellen periode van inactiviteit automatisch beëindigd. De externe gebruiker wordt geacht zich te onthouden van de toepassing van periodieke processen om de verbinding kunstmatig in stand te houden.

6. GEDRAGSCODE VOOR HET GEBRUIK VAN INTERNET

6.1 Het ziekenhuis verleent zijn bezoekers een tijdelijk, niet-exclusief en niet overdraagbaar recht om gratis wifi te gebruiken. De dienst ICT volgt het internetgedrag op dit publiek toegankelijk netwerk op en behoudt zich het recht om de toegang tot bepaalde sites of diensten te beperken of te weigeren.

6.2 De gebruikers-bezoekers verbinden zich ertoe om uitsluitend geschikte en behoorlijk functionerende apparatuur en software te gebruiken voor de gratis wifi. Zodra de gebruikers-bezoekers bemerken of redelijkerwijze dienen te bemerken dat de door hem/haar gebruikte apparatuur/software niet geschikt is voor aansluiting op de gratis wifi, niet behoorlijk functioneert of het gebruik of de werking van de gratis wifi of het netwerk belemmert of verstoort, dienen de gebruikers-bezoekers zijn/haar gebruik van de apparatuur stop te zetten.

7. TOEZICHT EN CONTROLE

7.1 Principes en controle

7.1.1 Externe medewerkers, leveranciers, dienstverleners en hun onderaannemers aanvaarden dat het ziekenhuis een controle uitvoert om eventuele onregelmatigheden m.b.t. het gebruik van zijn apparatuur en systemen op de sporen en om de naleving van de verplichtingen opgesomd in deze policy te controleren en dit binnen de wettelijke beperkingen met betrekking tot de volgende situaties:

7.1.1.1 de preventie van ongeoorloofde feiten of van feiten die indruisen tegen de goede zeden of die de waardigheid van andere personen kunnen aantasten;

7.1.1.2 de bescherming van de belangen van de instelling, onder meer tegen informatielekken of een verkeerd gebruik van de informatie;

7.1.1.3 de veiligheid en/of de goede technische werking van de functionerende informaticasystemen van de instelling.

8. SANCTIES

8.1.1 Voor externe medewerkers, leveranciers, dienstverleners en hun onderaannemers zal de juridische werkgever op de hoogte gesteld worden van de inbreuk en de eventuele tijdelijke of definitieve herroeping van de autorisatie tot gevolg hebben en aanleiding geven tot een verbod van toegang tot de gebouwen en toepassingen van het ziekenhuis betekenen.

8.1.2 Bij niet-nakoming door de externe medewerkers, leveranciers, dienstverleners en hun onderaannemers van de in deze annex opgenomen geheimhoudingsplicht is de juridische werkgever aan het ziekenhuis een direct opeisbare boete verschuldigd ten bedrage van 1500€ per gebeurtenis voor iedere dag dat de niet-nakoming aanhoudt. Naast deze vergoeding is het ziekenhuis vrij om alle schade hoger dan deze vergoeding te vorderen van de leverancier.

8.1.3 Indien de externe medewerkers, leveranciers, dienstverleners en hun onderaannemers zijn verplichtingen, voortvloeiend uit deze gedragscode niet, niet tijdig of niet naar behoren nakomt, is hij van rechtswege in gebreke.

ANNEX 3 - MODELFORMULIER MELDING GEGEVENSLEK DOOR VERWERKER

1.1. IDENTIFICATIE

1.1.1. VERWERKINGSVERANTWOORDELIJKE

- Telefoonnummer contact 24/7: 0497/58.89.54.

1.1.2. VERWERKER

- Bedrijfsnaam :
- Adres:
- Contactpersoon:
- Telefoonnummer contactpersoon 24/7:
- Mailadres:

1.1.3. WIE KAN BENADERD WORDEN VOOR MEER INFORMATIE OVER DE INBREUK?

- Contactpersoon:
- Telefoonnummer contactpersoon 24/7:
- Mailadres:

1.2. CONTEXT INBREUK

1.2.1. WIE HEEFT DE INBREUK GECONSTATEERD?

- Identificatie, naam:
- Functie/hoedanigheid:

1.2.2. TIJDSTIP

- Datum/tijd:

1.2.3. OMSCHRIJVING

- Omschrijf het beveiligingsincident waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan:
- Wanneer heeft de inbreuk plaatsgevonden?
    - Op (datum + tijd):
    - Tussen (datum + tijd) en (datum + tijd)
    - Is nog niet vastgesteld
    - Er is sprake van een anonieme melding door een derde

1.2.4. CATEGORIEËN VAN PERSOONSGEGEVENS WAAROP DE INBREUK VAN TOEPASSING IS

- Omschrijf:
    - 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) :

1.2.5. CATEGORIEËN VAN BETROKKENEN WAAROP DE INBREUK VAN TOEPASSING

- Omschrijf de groep mensen waarvan persoonsgegevens zijn betrokken bij de inbreuk:

1.3. IMPACT

1.3.1. HOEVEELHEID

- Van hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk?
    - Geen, de gegevens zijn niet herleidbaar tot een individu
    - Nog niet vastgesteld
    - Ten minste ……(aantal), maar niet meer dan ……aantal) betrokkenen
- Heeft de inbreuk betrekking op personen uit andere EU-landen?

1.3.2. OMSTANDIGHEDEN

- De data konden worden bekeken:
- De data konden worden gekopieerd:
- De data konden worden gewijzigd/gewist/verwijderd:
- Nog niet gekend:

1.4. BEVEILIGING EN MAATREGELEN

1.4.1. VERSLEUTELING

- Zijn de Persoonsgegevens versleuteld? Zo ja hoe?

1.4.2. BEWARENDE MAATREGELEN

- Welke beveiligingsmaatregelen (technisch en organisatorisch) zijn getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen?