

## ADDENDUM LEVERANCIERSOVEREENKOMST M.B.T. INFORMATIEVEILIGHEID

### Tussen ondergetekenden

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 ..... **[naam]**, algemeen directeur, Hierna genoemd "**het Ziekenhuis**"

EN

.....

.....

..... **[gegevens Leverancier aan te vullen]**

Hierna genoemd "**Leverancier**"

Hierna gezamenlijk genoemd de "**Partijen**"

### Overwegende dat

De Leverancier diensten verricht ten behoeve van het Ziekenhuis, zoals beschreven in de Basisovereenkomst, deze diensten een mogelijke impact kunnen hebben op de beveiliging van informatie en systemen en de partijen met dit Addendum de afspraken wensen vast te leggen over de nodige organisatorische en technische maatregelen om een passend niveau van informatieveiligheid te waarborgen.

**wordt overeengekomen als volgt:**

## 1. BEGRIPPENKADER

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

- **NIS2-wetgeving:** Wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid. Deze wet wordt doorgaans de Belgische NIS2-wet genoemd. Zij zet de Europese NIS2-richtlijn (EU) 2022/2555 om in Belgisch recht.

- **Basisovereenkomst: de overeenkomst tussen het Ziekenhuis en de Leverancier van**

.....[datum]

met betrekking tot

.....

.....[invullen titel overeenkomst, evt. referentienummer]

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

## 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 informatiesystemen die de Leverancier ter beschikking stelt in het kader van de uitvoering van de diensten in de Basisovereenkomst.

2.2 De bepalingen uit dit Addendum (en Annexen) gaan voor op de (eventueel andersluidende) bepalingen over informatieveiligheid in de Basisovereenkomst en vervangen deze.

## 3. PASSENDE TECHNISCHE EN ORGANISATORISCHE MAATREGELEN

### Doel en normatief kader

3.1 De Leverancier implementeert en onderhoudt passende en evenredige organisatorische maatregelen (naast technische en operationele maatregelen) om risico's voor de beveiliging van netwerk- en informatiesystemen, en de impact van incidenten op de zorgcontinuïteit en geleverde zorgdiensten, te voorkomen of te minimaliseren, overeenkomstig Titel 3, Hoofdstuk 1 (Art. 30-33) van de Belgische NIS2-wet.

3.2 Deze maatregelen volgen een alomvattende risicobenadering en dekken minstens de elementen uit de Belgische NIS2-wet (transpositie van NIS2 Art. 21), waaronder: (a) beleid voor risicoanalyse en informatiebeveiliging; (b) incidentafhandeling; (c) bedrijfscontinuïteit (back-up, disaster recovery, crisismanagement); (d) beveiliging van de toeleveringsketen; (e) beveiliging bij aanschaf, ontwikkeling en onderhoud (incl. kwetsbaarhedenbeheer en melding); (f) beleid en procedures voor effectiviteitsmeting; (g) cyberhygiëne en training; (h) cryptografie/encryptie; (i) personeelsbeveiliging, toegangsbeheer en activabeheer; (j) multifactorauthenticatie en beveiligde communicatie.

### **Zorgplicht in de keten (supplychain security)**

- 3.3** De Leverancier waarborgt dat onderaannemers en kritieke leveranciers voor de geleverde diensten ten minste gelijkwaardige NIS2-conforme maatregelen toepassen, met contractuele doorwerking (flowdown), voorschrijft tot tijdige incidentmelding aan de Leverancier, en audit- en bewijsplicht aan het Ziekenhuis.
- 3.4** De Leverancier houdt een actueel leveranciersregister bij met risicoclassificatie, beveiligingseisen en resultaten van periodieke beoordelingen (minstens jaarlijks), en stelt dit op verzoek ter beschikking aan het Ziekenhuis voor doeleinden inzake NIS2-compliance.

### **Beleidskader, governance en opleiding**

- 3.5** De Leverancier onderhoudt aantoonbaar formele, actuele beleidsdocumenten (ISMS-beleid, risicobeheerbeleid, incident- en crisisprocedures, BCM/DR-plannen, kwetsbaarhedenbeheer, patchbeleid, encryptiebeleid, identiteits- en toegangsbeheerbeleid, gegevensklassificatie).
- 3.6** De Leverancier voorziet rolgebaseerde opleidingen en regelmatige sensibilisering voor alle betrokken personeelsleden en in het bijzonder voor beheerders/ geprivilegieerde gebruikers, conform de training en cyberhygiënevereisten uit Titel 3, Hoofdstuk 1 artikel 30 van de NIS2 wetgeving.

### **Identiteit en toegangsbeheer (IAM) en privileged access**

- 3.7** Sterke authenticatie (MFA) is verplicht voor alle beheerdersaccounts, externe toegang en alle toegang tot productie en zorgkritische systemen. Het principe van minimale privileges en functiescheiding vormt het uitgangspunt.
- 3.8** Logging & monitoring van beveiligingsrelevante gebeurtenissen is ingericht (SIEM/gelijkaardig), met minimale retentie van 12 maanden voor PAM-sessies en correlatie met detectie en responscapaciteiten. (Deze retentie is een contractspecificatie ten behoeve van verantwoording en forensisch onderzoek).

### **Encryptie en gegevensbescherming**

- 3.9** Versleuteling in rust en tijdens transport is verplicht voor zorgkritische gegevens. Sleutelbeheer is gedocumenteerd en gescheiden van operationele beheerkanalen.
- 3.10** Bij incidenten en crisissituaties gebruikt de Leverancier voor spraak/video/tekst en noodcommunicatie beveiligde communicatiekanalen.

### **Kwetsbaarhedenbeheer en veilige ontwikkeling**

- 3.11** De Leverancier hanteert een geformaliseerd proces voor kwetsbaarhedenbeheer (identificatie, prioritering volgens risico, bekende actief misbruikte kwetsbaarheden, patching binnen gedefinieerde termijnen) en het melden van kwetsbaarheden.
- 3.12** Bij softwareontwikkeling levert de Leverancier “secure by design” en “secure by default” op, inclusief change- en releasemanagement met gescheiden omgevingen, code-reviews en (indien van toepassing) SBoM-beschikbaarheid voor het Ziekenhuis.

## **Bedrijfscontinuïteit, back-up en crisismanagement**

**3.13 BCP/DRP** zijn door de Leverancier afgestemd op de dienstverlening van het Ziekenhuis. Er wordt minimaal jaarlijks één test (incl. tabletopoefening met het Ziekenhuis) uitgevoerd, met hersteldoelstellingen (RTO/RPO) die de continuïteit van de zorg waarborgen en conform de BCM-verplichting uit Titel 3, Hoofdstuk 1 artikel 30.

**3.14 Back-ups** van de Leverancier zijn versleuteld, offline/persistent waar relevant, en periodiek getest op herstelbaarheid.

## **INCIDENTMANAGEMENT en meldingsondersteuning (contractueel, ter ondersteuning van NIS2 meldplicht)**

**3.15** De Leverancier heeft een 24/7-incidentresponsproces met aanspreekpunt en communicatiekanalen voor het Ziekenhuis.

**3.16** Interne meldtermijnen aan het Ziekenhuis (contractueel):

- **Binnen 4 uur:** eerste waarschuwing met kerngegevens (wat, wanneer, scope, voorlopige impact, genomen eerste maatregelen).
- **Binnen 24 uur:** update met indicatie oorzakelijkheid (al dan niet kwaadwillig), potentiële grensoverschrijdende impact en eerste indicatoren van compromittering (indien beschikbaar), zodat het Ziekenhuis – als essentiële entiteit – tijdig kan voldoen aan de vroegtijdige waarschuwing binnen 24 uur van de Belgische NIS2-wet (Art. 34) en de 72-uursincidentmelding (Art. 35), in lijn met de NIS2-rapportagesystematiek.
- **Binnen 1 maand na de initiële melding of beëindiging van het incident:** eindrapport met grondoorzaak, impactanalyse, toegepaste en geplande mitigaties, en geleerde lessen.
- De Leverancier verleent volledige medewerking bij coördinatie met het CCB/CERT.be indien het Ziekenhuis beslist tot (vrijwillige of verplichte) nationale melding, met inbegrip van het delen van relevante technische artefacten. (Het CCB is als nationale cyberbeveiligingsautoriteit en nationaal CSIRT aangeduid bij het KB van 9 juni 2024.)

## **4. AANTOONBAARHEID, CONFORMITEIT EN AUDITS**

Ter aantoonbaarheid van conformiteit met artikel 3 levert de Leverancier één of meer van onderstaande bewijzen aan:

- CCB CyberFundamentals (CyFun®) label op relevant niveau, of
- ISO/IEC 27001-certificaat met scope die de geleverde diensten en verwerkingen voor het Ziekenhuis dekt, inclusief Statement of Applicability, of
- een equivalente conformiteitsbeoordeling volgens het KB 9 juni 2024 (erkende CAB), of
- een recente, onafhankelijke assurance-rapportering (bv. ISAE 3000/3402 type 2) met voldoende dekking van de in artikel 3 genoemde maatregelen.
- Ingevulde zelfevaluatievragenlijst in Annex 1

Het Ziekenhuis heeft het recht om (zelf of via een onafhankelijke derde) audits en/of penetratietests te laten uitvoeren op redelijke wijze, mits redelijke kennisgeving en met inachtneming van vertrouwelijkheid, teneinde de naleving van dit artikel te verifiëren. De Verwerker werkt hieraan mee en remedieert geconstateerde tekortkomingen binnen redelijke termijnen. (Dit sluit aan bij de regelmatige conformiteitsbeoordelingen uit Titel 4 van de NIS2-wet en het uitvoerings-KB.)

## **5. DOCUMENTATIE EN INFORMATIEVERSTREKKING AAN HET ZIEKENHUIS/AUTORITEITEN**

- 5.1** Op verzoek verstrekt de Leverancier actuele documentatie (risicoregisters, assetinventaris, netwerkdiagrammen op hoog niveau, BCM/DR testverslagen, opleidingsregisters, auditrapporten) die nodig zijn voor de NIS2-verplichtingen van het Ziekenhuis (o.m. toezicht en inspectie door CCB).
- 5.2** Indien de Leverancier zelf binnen het toepassingsgebied van de Belgische NIS2-wet valt, bevestigt hij registratie bij het CCB en deelt hij op verzoek relevante referenties mee (registratie ID, aangewezen sector/subsector).

## **6. CLOUDPROVIDER EN CLOUDDIENSTEN (INDIEN VAN TOEPASSING)**

Als de Leverancier clouddiensten inzet of zelf clouddiensten levert ter ondersteuning van de dienstverlening aan het Ziekenhuis, waarborgt de Leverancier dat de cloudopzet en keten voldoen aan de verplichtingen inzake risicobeheer, bedrijfscontinuïteit en supply-chain-beveiliging onder de NIS2-wet.

De Leverancier bezorgt het Ziekenhuis een actueel overzicht van gebruikte clouddiensten (IaaS/PaaS/SaaS), cloudprovider(s), relevante componenten (identiteitsbeheer, logging, backup/DR), datageografie/regio's en een "gedeelde verantwoordelijkheid matrix".

De Leverancier past voor cloudbeheer minstens toe: MFA, least privilege, logging van admin-activiteiten en change control.

Cloudincidenten bij de cloudprovider die de dienstverlening aan het Ziekenhuis beïnvloeden vallen onder de meldings- en samenwerkingsafspraken van artikel 3.

### **6.1 Bescherming van gegevens (Data Protection)**

#### **6.1.1 Data in rust (Data at Rest)**

- 6.1.1.1 De Leverancier zorgt ervoor dat alle gegevens die door of namens het Ziekenhuis worden opgeslagen, worden permanent versleuteld opgeslagen.
- 6.1.1.2 Ontsleuteling van deze gegevens is uitsluitend toegestaan binnen een beveiligde, geïsoleerde uitvoeringsomgeving (confidential computing omgeving).
- 6.1.1.3 Gegevens worden vóór het verlaten van deze uitvoeringsomgeving opnieuw volledig versleuteld.
- 6.1.1.4 Gegevens mogen de omgeving op geen enkel moment in leesbare vorm verlaten.

#### **6.1.2 Data tijdens transport (Data in Transit)**

- 6.1.2.1 De Leverancier zorgt ervoor dat alle overdracht van gegevens tussen systemen, componenten en diensten uitsluitend plaats vindt via sterk beveiligde en versleutelde communicatiekanalen.
- 6.1.2.2 Ontsleuteling tijdens transport is uitsluitend toegestaan binnen een vertrouwelijke uitvoeringsomgeving.
- 6.1.2.3 Overdracht van gegevens in niet versleutelde of leesbare vorm over cloudnetwerken is uitdrukkelijk verboden.

#### **6.1.3 Beveiligde gegevensuitwisseling met het cloudplatform**

- 6.1.3.1 De communicatie tussen de cloudapplicatie van het Ziekenhuis en het cloudplatform van de Leverancier moet zodanig zijn ingericht dat vertrouwelijkheid, integriteit en authenticiteit van de informatie gewaarborgd blijven gedurende de volledige levenscyclus van de gegevens.

## **6.2 Encryptiesleutels, secrets en authenticatiemiddelen**

### **6.2.1 Bescherming van encryptiesleutels en secrets**

- 6.2.1.1 Encryptiesleutels en andere secrets worden uitsluitend gegenereerd, opgeslagen en gebruikt binnen een beveiligde omgeving.
- 6.2.1.2 Encryptiesleutels en secrets mogen de enclave nooit in leesbare of herbruikbare vorm verlaten.
- 6.2.1.3 De Leverancier heeft geen technische, logische of operationele mogelijkheid om deze encryptiesleutels of secrets te raadplegen of te extraheren.

### **6.2.2 Onafhankelijk sleutelbeheer**

- 6.2.2.1 Het beheer van encryptiesleutels en secrets gebeurt op een systeem waartoe de Leverancier geen toegang heeft.
- 6.2.2.2 Dit systeem mag niet worden beheerd, gemonitord of ondersteund door de Leverancier.

### **6.2.3 Authenticatiemiddelen**

- 6.2.3.1 Authenticatiemiddelen (zoals wachtwoorden, tokens, certificaten en sleutels) worden beschouwd en behandeld als secrets.
- 6.2.3.2 De Leverancier heeft geen toegang tot systemen die authenticatiemiddelen beheren of authenticatie uitvoeren.

## **6.3 Toegangsbeheer en identiteit**

### **6.3.1 Beperkingen voor de Leverancier**

- 6.3.1.1 De Leverancier heeft geen logische toegang tot servers, virtuele machines of enclaves waarin gegevens van het Ziekenhuis worden verwerkt.
- 6.3.1.2 Deze beperking geldt ook voor beheeraccounts, noodaccounts en interne authenticatiemiddelen van de Leverancier.

### **6.3.2 Authenticatie en autorisatie**

- 6.3.2.1 De cloudapplicatie maakt verplicht gebruik van multifactorauthenticatie (MFA).
- 6.3.2.2 Toegangsbeheer gebeurt via koppeling met Azure Active Directory of een gelijkwaardig identiteitsplatform onder controle van het Ziekenhuis.
- 6.3.2.3 De Leverancier heeft geen toegang tot systemen die autorisaties definiëren of afdwingen.

## **6.4 Verwijdering van gegevens**

- 6.4.1 De Leverancier garandeert dat gegevens volledig en onomkeerbaar worden verwijderd van alle storage wanneer het Ziekenhuis hiertoe opdracht geeft.
- 6.4.2 Deze verwijderingsprocedures worden regelmatig geverifieerd en geattesteerd door een onafhankelijke externe partij.
- 6.4.3 De resultaten van deze attestaties worden op verzoek ter beschikking gesteld van het Ziekenhuis.

## **6.5 Exitstrategie en beëindiging van de dienstverlening**

### **6.5.1 Doel van de exitstrategie**

De exitstrategie heeft tot doel te waarborgen dat het Ziekenhuis, bij beëindiging of wijziging van de dienstverlening, zijn gegevens en applicaties veilig, volledig en zonder onredelijke belemmeringen kan blijven gebruiken of kan migreren naar een andere dienstverlener of naar een eigen infrastructuur, met behoud van vertrouwelijkheid, integriteit en beschikbaarheid.

### **6.5.2 Exit-scenario's**

De exitstrategie is van toepassing in elk van de volgende gevallen:

- beëindiging of niet-verlenging van de overeenkomst, ongeacht de oorzaak;
- een materiële contractbreuk door de Leverancier;
- wijzigingen aan de dienstverlening die een onaanvaardbaar risico vormen voor de beveiliging of wettelijke conformiteit;
- faillissement, stopzetting of overdracht van (een deel van) de activiteiten van de Leverancier;
- wettelijke of regulatorische verplichtingen die een migratie of beëindiging vereisen.

### **6.5.3 Overdraagbaarheid van gegevens en configuraties**

6.5.3.1 De Leverancier stelt het Ziekenhuis in staat om alle gegevens, metadata, configuraties en logische structuren die noodzakelijk zijn voor voortzetting van de dienstverlening, op een gestructureerde, gangbare en machine leesbare wijze te verkrijgen.

6.5.3.2 De Leverancier zorgt ervoor dat de gegevens worden aangeleverd in een formaat dat migratie naar een alternatief platform technisch mogelijk maakt zonder verlies van functionaliteit of gegevensintegriteit.

6.5.3.3 De Leverancier zorgt ervoor dat de overdracht plaatsvindt via beveiligde en versleutelde mechanismen die gelijkwaardig zijn aan de beveiligingsmaatregelen tijdens de looptijd van de overeenkomst.

### **6.5.4 Beveiliging tijdens de exitfase**

6.5.4.1 Tijdens de volledige exitfase blijven alle contractueel overeengekomen beveiligingsmaatregelen onverkort van toepassing.

6.5.4.2 Gegevens worden ook tijdens migratie en overdracht uitsluitend versleuteld verwerkt en getransporteerd.

6.5.4.3 Encryptiesleutels, secrets en authenticatiemiddelen blijven te allen tijde onder exclusieve controle van het Ziekenhuis en worden niet aan de Leverancier overgedragen.

### **6.5.5 Ondersteuning door de Leverancier**

6.5.5.1 De Leverancier verleent redelijke en tijdige ondersteuning bij de uitvoering van de exitstrategie, inclusief:

- beschikbaarstelling van documentatie;
- technische ondersteuning bij export en migratie;
- beantwoording van vragen met betrekking tot gegevensstructuren en afhankelijkheden.

6.5.5.2 Deze ondersteuning mag niet afhankelijk worden gesteld van aanvullende commerciële voorwaarden die de uitvoering van de exit onredelijk vertragen of belemmeren.

### **6.5.6 Verwijdering van gegevens na exit**

6.5.6.1 Na succesvolle en volledige overdracht van de gegevens bevestigt de Leverancier schriftelijk dat alle gegevens van het Ziekenhuis onomkeerbaar zijn verwijderd uit zijn systemen, inclusief back-ups en redundante opslag.

6.5.6.2 Deze verwijdering gebeurt binnen een overeengekomen termijn en volgens aantoonbaar veilige procedures.

6.5.6.3 Op verzoek van het Ziekenhuis verstrekt de Leverancier een verklaring of attest waaruit blijkt dat de verwijdering effectief is uitgevoerd.

### **6.5.7 Continuïteit en beschikbaarheid**

6.5.7.1 De Leverancier waarborgt dat gedurende de exitperiode de beschikbaarheid van de dienstverlening niet zonder geldige reden wordt verminderd.

6.5.7.2 De exitstrategie mag geen aanleiding geven tot onverwachte onderbrekingen of verlies van toegang tot gegevens, behoudens wanneer dit strikt noodzakelijk is voor de veilige uitvoering van de exit.

**6.5.8** Periodieke toetsing

6.5.8.1 Het Ziekenhuis heeft het recht om de uitvoerbaarheid van de exitstrategie periodiek te laten toetsen.

6.5.8.2 De Leverancier verleent medewerking aan dergelijke toetsen, waaronder het uitvoeren van een gecontroleerde exit- of migratiesimulatie indien dit redelijkerwijze kan worden verwacht.

**6.5.9** Voorrang en afdwingbaarheid

6.5.9.1 De bepalingen van dit artikel hebben voorrang op tegenstrijdige exit- of beëindigingsbepalingen in andere documenten.

6.5.9.2 Het niet naleven van dit artikel wordt beschouwd als een wezenlijke tekortkoming in de nakoming van de overeenkomst.

**7. ARTIFICIËLE INTELLIGENTIE (INDIEN VAN TOEPASSING)**

Als de Leverancier AI inzet of zelf AI-diensten levert ter ondersteuning van de dienstverlening aan het Ziekenhuis, waarborgt de Leverancier dat de AI-componenten voldoen aan de verplichtingen van de AI Act. Indien van toepassing moet de vragenlijst uit Annex 2 worden beantwoord.

Aldus overeengekomen en in tweevoud opgemaakt te .....  
op .....

[Naam]

**Het Ziekenhuis**

[Naam]

**Leverancier**

**Annexen**

Annex 1: De informatieveiligheid – zelfevaluatievragenlijst

Annex 2: Vragenlijst voor aankoopdossiers met AI-component

## ANNEX 1 – DE INFORMATIEVEILIGHEID – ZELFEVALUATIEVRAGENLIJST

### VRAGENLIJST INZAKE AANWEZIGHEID EN EFFECTIVITEIT VAN DE ORGANISATORISCHE EN TECHNISCHE MAATREGELEN VOOR INFORMATIEVEILIGHEID

In te vullen door de Leverancier

Beantwoord elke vraag en vermeld (met titel) welke stavingsstukken u ter beschikking houdt.

De antwoorden op de vragen moeten ook betrekking hebben op de verwerkingen door onderaannemers.

| VRAGEN                                                                                                                                                                                                | NEE | JA | GETEST | STAVINGSSTUKKEN | Korte uitleg |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----|--------|-----------------|--------------|
| <b>Beschrijving van de dienst</b>                                                                                                                                                                     |     |    |        |                 |              |
| Is de documentatie inzake de geleverde dienst actueel en accuraat?                                                                                                                                    |     |    |        |                 |              |
| <b>Organisatorische Maatregelen</b>                                                                                                                                                                   |     |    |        |                 |              |
| <b>ISO 5.1</b> – Is er een duidelijke security policy die alle domeinen van de ISO 27001/27002 afdekt rekening houdende met beschreven “te beschouwen dimensies” en is dit bekend bij de medewerkers? |     |    |        |                 |              |
| <b>ISO 5.2</b> – Zijn de rollen en verantwoordelijkheden vastgelegd met name inzake CISO, DPO, operationeel beheer, incidentenbeheer?                                                                 |     |    |        |                 |              |
| <b>ISO 5.3</b> – Is functiescheiding toegepast om ongeoorloofde acties onmogelijk te maken?                                                                                                           |     |    |        |                 |              |
| <b>ISO 5.4</b> – Is het informatieveiligheidsbeleid formeel goedgekeurd en wordt het periodiek herzien door het management?                                                                           |     |    |        |                 |              |
| <b>ISO 5.7</b> – Wordt er gebruikgemaakt van gestructureerde dreigingsanalyses om de informatieveiligheid te waarborgen?                                                                              |     |    |        |                 |              |
| <b>ISO 5.8</b> – Wordt informatiebeveiliging mee opgenomen in het projectmanagement?                                                                                                                  |     |    |        |                 |              |
| <b>ISO 5.10</b> – Is er een beleid rond aanvaardbaar gebruik van informatie en gebruiksmiddelen?                                                                                                      |     |    |        |                 |              |

|                                                                                                                                                                                                                            |  |  |  |  |  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|--|--|
| <b>ISO 5.12/5.13</b> – Wordt er een classificatie van data en van systemen toegepast?                                                                                                                                      |  |  |  |  |  |
| <b>ISO 5.14</b> – Welke formele regels en technische maatregelen hanteren jullie om informatie veilig en traceerbaar uit te wisselen met zowel interne als externe partijen?                                               |  |  |  |  |  |
| <b>ISO 5.15/5.16/5.17/5.18</b> – Is er een strikt gebruikers- en toegangsbeheer? Zowel voor gewone gebruikers als voor geprivilegieerde beheerders?                                                                        |  |  |  |  |  |
| <b>ISO 5.19</b> – Worden de contractuele verplichtingen 1-op-1 doorgezet naar uw onderaannemers en houdt u daar minimaal jaarlijks toezicht op?                                                                            |  |  |  |  |  |
| <b>ISO 5.20</b> – Worden alle belangrijke activiteiten (met name van beheerders) in onwijzigbare audittrails vastgelegd die toegankelijk zijn voor het Ziekenhuis?                                                         |  |  |  |  |  |
| <b>ISO 5.21/5.22/5.23</b> – Hebt u duidelijke regels inzake levering en gebruik van software en hardware en (security) testing – toepasselijk voor elke wijziging?                                                         |  |  |  |  |  |
| <b>ISO 5.24</b> – Is er een beleid en zijn er duidelijke systemen en processen voor het beheren (en coördineren) van veiligheidsincidenten?                                                                                |  |  |  |  |  |
| <b>ISO 5.29 / ISO 5.30</b> – Heeft u een planning voor de continuïteit van informatiebeveiliging in geval van een ramp/verstoring en worden deze ook getest?                                                               |  |  |  |  |  |
| <b>ISO 5.31</b> – Beschikt de organisatie over een actueel en gedocumenteerd overzicht van alle relevante wettelijke, regelgevende en contractuele beveiligingseisen en wordt de naleving hiervan periodiek gecontroleerd? |  |  |  |  |  |
| <b>ISO 5.32</b> – Hanteert de organisatie gedocumenteerde procedures om intellectuele-eigendomsrechten te beschermen en het gebruik van illegale software of ongeautoriseerde kopieën te voorkomen?                        |  |  |  |  |  |

|                                                                                                                                                                                                                  |  |  |  |  |  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|--|--|
| <b>ISO 5.34</b> – Kent u de regels inzake privacybescherming en bescherming van persoonsgegevens en past u die toe?                                                                                              |  |  |  |  |  |
| <b>ISO 5.35</b> – Wordt er onafhankelijk geverifieerd of de informatiebeveiliging voldoet aan de gestelde beveiligingseisen (bijv. middels interne audit, externe audit)?                                        |  |  |  |  |  |
| <b>ISO 5.36</b> – Hoe wordt de naleving van beleid, regels en normen voor informatiebeveiliging gewaarborgd?                                                                                                     |  |  |  |  |  |
| <b>Personele Maatregelen</b>                                                                                                                                                                                     |  |  |  |  |  |
| <b>ISO 6.1 / 6.2 / 6.3</b> – Zijn er duidelijke regels en is er toezicht op gedrag van geprivilegieerde beheerders? En worden veiligheidsregels jaarlijks herhaald in hun training?                              |  |  |  |  |  |
| <b>ISO 6.3</b> – Worden medewerkers structureel getraind en geïnformeerd over de risico's en het veilig omgaan met informatie?                                                                                   |  |  |  |  |  |
| <b>ISO 6.4/6.5/6.6</b> – Zijn er duidelijke regels in geval van non-compliant gedrag? Bij het veranderen van functie of verlaten van de firma? Zijn al uw medewerkers gebonden door een geheimhoudings-clausule? |  |  |  |  |  |
| <b>ISO 6.7 / 6.8</b> – Zijn er duidelijke regels inzake werken op afstand (enkel middels systemen van de verwerker) + het rapporteren van eventuele/mogelijke veiligheidsincidenten?                             |  |  |  |  |  |
| <b>Fysieke Maatregelen</b>                                                                                                                                                                                       |  |  |  |  |  |
| <b>ISO 7.1/7.2/7.3/7.4</b> – Zijn de toegang tot de systemen en de systemen die gebruikt worden bij beheer op niveau?                                                                                            |  |  |  |  |  |
| <b>ISO 7.5/7.6/7.7/7.8/7.10/7.11</b> – Zijn adequate maatregelen getroffen die ongeautoriseerde toegang tot systemen en dragers van data in principe onmogelijk maken?                                           |  |  |  |  |  |

|                                                                                                                                                                                                                     |  |  |  |  |  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|--|--|
| <b>ISO 7.14</b> – Wordt er gebruik gemaakt van cryptografische vernietiging of fysieke vernietiging om te garanderen dat data definitief verwijderd is en /of de hardware vernietigd?                               |  |  |  |  |  |
| <b>Technologische Maatregelen</b>                                                                                                                                                                                   |  |  |  |  |  |
| <b>ISO 8.1</b> – Wordt alle informatie die is opgeslagen op, verwerkt door of toegankelijk via user endpoint devices (laptops, smartphones en tablets) adequaat beschermd conform het informatiebeveiligingsbeleid? |  |  |  |  |  |
| <b>ISO 8.2 / ISO 8.3 / ISO 8.4</b> – Hebt u een aparte privileged access management omgeving (PAM)? Wordt voor (beheers)toegang op afstand gebruik gemaakt van een VPN? En is toegang beperkt tot een need-to-know? |  |  |  |  |  |
| <b>ISO 8.5</b> – Past u sterke authenticatie toe op al uw processen en MFA voor alle geprivilegieerde toegangen?                                                                                                    |  |  |  |  |  |
| <b>ISO 8.7 / 8.8</b> – Zijn uw systemen maximaal beschermd tegen malware? Test u uw systemen adequaat tegen kwetsbaarheden?                                                                                         |  |  |  |  |  |
| <b>ISO 8.10 / 8.11 / 8.12 / 8.13</b> – Beschermt u data adequaat en conform hun CIA-classificatie-niveaus?                                                                                                          |  |  |  |  |  |
| <b>ISO 8.14</b> – Beschikt u conform de CIA-classificatie over de nodige back-up en disaster recovery systemen?                                                                                                     |  |  |  |  |  |
| <b>ISO 8.15/8.16</b> – Beschikt u over adequate logging en monitoring om security incidenten te kunnen detecteren?                                                                                                  |  |  |  |  |  |
| <b>ISO 8.19</b> – heeft u een beveiligingsbeleid voor het downloaden en installeren van software?                                                                                                                   |  |  |  |  |  |
| <b>ISO 8.20 / 8.21 / 8.22</b> – Is er een beleid voor toegang tot netwerken en netwerkservices en is uw infrastructuur opgezet volgens de regels van de kunst om data en systemen adequaat genoeg te scheiden?      |  |  |  |  |  |

|                                                                                                                                                              |  |  |  |  |  |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|--|--|--|
| <b>ISO 8.24</b> – Past u waar nodig adequate cryptografische maatregelen toe zoals signing of encryptie?                                                     |  |  |  |  |  |
| <b>ISO 8.25 / 8.26 / 8.27 / 8.28 / 8.29</b> – Heeft u een software delivery pipeline die elke code-/config-wijziging valideert op fouten/non-conformiteiten? |  |  |  |  |  |
| <b>ISO 8.33</b> – Heeft u een beleid om testgegevens te beschermen en anoniem te maken?                                                                      |  |  |  |  |  |

|                                                                                                                                                                  |              |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| De Leverancier,                                                                                                                                                  |              |
| Naam en functie van de persoon die tekent namens de Leverancier<br>( <i>wettelijke vertegenwoordiger</i> )                                                       |              |
| Datum                                                                                                                                                            |              |
| Ik verklaar dat de antwoorden juist zijn en geen belangrijke tekortkomingen verhullen.<br>Ik verplicht mij om de stavende stukken te overhandigen bij een audit. | Handtekening |

## ANNEX 2 – VRAGENLIJST VOOR AANKOOPDOSSIERS MET AI-COMPONENT

Aangezien het Ziekenhuis moet voldoen aan de AI-wet- en regelgeving (o.a. de AI Act in Europa) én steeds een grondige evaluatie moet maken van alle AI-toepassingen in de zorgomgeving, wordt u gevraagd om onderstaande vragen in te vullen. Dit geeft het Ziekenhuis een eerste, high-level inzicht in de AI-functionaliteit van het product en/of software.

Maak in uw antwoorden waar relevant het onderscheid tussen data gebruikt voor het trainen van het model en data gebruikt in de toepassing.

### 1. Type AI-functionaliteit

- Kunt u aangeven of en in welke mate het product gebruikmaakt van AI/zelflerende algoritmes?
- Wat is de kernfunctionaliteit die door het AI-systeem wordt uitgevoerd (diagnostiek, workflow-optimalisatie, besluitvorming, monitoring, beeldherkenning, enz.)?
- Is jullie AI-systeem gebaseerd op een AI-model voor algemene doeleinden dat in staat is om een breed scala aan verschillende taken competent uit te voeren? Dit geldt niet als u AI-modellen van derden gebruikt.  
Voorbeelden van AI-modellen voor algemeen gebruik zijn:
  - Grote taalmodellen (LLM's).
  - Tekst-naar-beeld- of tekst-naar-videomodellen.
  - Grote visusmodellen.
  - Multimodale modellen?
- Welke data van het Ziekenhuis gebruikt het AI-systeem (cfr overzicht in de bijgevoegde Tabel 1)
- Tot welke categorie behoort het AI-systeem volgens de AI Act?
  - (Onaanvaardbaar)
  - Hoog risico
  - Beperkt risico
  - Geen risico

### 2. Werking en training van het AI-systeem

- Kan het AI-systeem of de Leverancier uitleggen hoe beslissingen of outputs tot stand zijn gekomen, met alle relevante stappen die het doorloopt en op welke informatie het systeem zich baseert? (cfr transparantieplichtingen onder de EU AI Act)
- Op welke data is de AI getraind (bijvoorbeeld: type patiëntgegevens, demografische gegevens, beeldmateriaal)? Is deze training specifiek gebaseerd op Europese of internationale datasets?
- Wordt het AI-systeem continu bijgestuurd (zelflerend) of gaat het om een statisch getraind model?
- Zo ja, worden de gegevens van het Ziekenhuis of van patiënten van het Ziekenhuis gebruikt om het AI-algoritme bij te sturen?
- Welke beperkingen heeft het AI-systeem? Probeer specifiek te zijn.

### 3. Kill switch en veiligheid

- Is er een kill switch / moet het Ziekenhuis het AI-systeem ook gebruiken als het dat niet wilt? Geeft de bijgevoegde documentatie aan hoe er kan overgeschakeld worden op een alternatief proces?
- Hoe wordt de nauwkeurigheid en validatie gegarandeerd en eventuele bias in de AI-uitkomsten voorkomen? Is hierover documentatie beschikbaar?
- Bestaat er documentatie over klinische validatiestudies of CE-markering (indien relevant)?
- Bestaat er certificatie voor het AI-systeem? vb. NIST
- Welke maatregelen zijn geïmplementeerd om te voorkomen dat het AI-systeem schadelijke, misleidende of klinisch onveilige output produceert?
- Hoe beschermen jullie het AI-systeem tegen AI-beveiligingsrisico's, zoals model poisoning of prompt injection-aanvallen?

#### 4. Risico's en risicoclassificatie

- Is het product reeds ingedeeld in een bepaalde risicoklasse onder de AI Act of onder de medische hulpmiddelenwetgeving (MDR)?
- Welke klasse is dit, hoe wordt dit gemotiveerd en is er bijbehorende documentatie?
- Welke risicobeperkende maatregelen worden er genomen, o.a. verzekering, uitsluiting van bepaalde data, beperking van bepaalde verwerkingen, etc?
- "Beschrijf de exitprocedure: welke stappen zijn voorzien om bij contractbeëindiging onze data (en – indien relevant – AI-modellen) terug te krijgen in een bruikbaar formaat?"
- "Ondersteunt u export en overdraagbaarheid van data of configuraties in gestructureerde, machineleesbare formaten?"

#### 5. Dataopslag en -bescherming

- Hoe gaan jullie om met privacy en gegevensbescherming in relatie tot AI?
- Kan bevestigd worden dat jullie geen AI zullen toepassen op onze gegevens of die van patiënten zonder onze uitdrukkelijke toestemming?
- Kan bevestigd worden dat geen van de gegevens van patiënten of van het Ziekenhuis worden gebruikt om het AI-systeem te trainen?

#### 6. Integratie en gebruik in de workflow

- Hoe is de AI-gebaseerde functie geïntegreerd in de dagelijkse praktijk (bijvoorbeeld: als beslissingsondersteuning in het EPD, zelfstandig toestel, enz.)?
- Is er een opleiding of begeleiding voorzien voor de verantwoordelijken voor de toepassing en voor de eindgebruikers, en hoe wordt die georganiseerd?

#### 7. Implementatie, testing, onderhoud en updates

- Wie is hiervoor verantwoordelijk?
- Kan het AI-model worden aangepast aan onze specifieke behoeften? Wie zou dit doen en hoe zouden de kosten/SLA eruitzien?
- Is er een mechanisme voor human oversight geïmplementeerd?
  - Wordt het AI-systeem zodanig ontworpen dat menselijke tussenkomst mogelijk blijft vóór beslissingen met kritieke gevolgen?
  - Zijn er waarborgen dat human oversight ook effectief kan worden uitgeoefend (bv. duidelijke uitleg, tijdige waarschuwingen, override-mogelijkheden)?
- Welk type ondersteuning bieden jullie aan gebruikers om de AI-functionaliteiten effectief te gebruiken?
- Op welke wijze worden updates of nieuwe versies van het AI-algoritme uitgerold en gecommuniceerd?
- Wordt er een proces voorzien om (eventuele) problemen of incidenten te melden en op te volgen?

Graag ontvangt het Ziekenhuis uw antwoorden op deze vragen om een eerste inschatting te kunnen maken. Op basis hiervan kan het Ziekenhuis beoordelen of het noodzakelijk is om een diepgaandere risicoanalyse, inclusief een formele AI-risk assessment, te starten.

Tabel 1: overzicht mogelijke gegevens

| Patiënt                                             |
|-----------------------------------------------------|
| Patiëntengegevens in het EPD                        |
| Administratieve identificatiegegevens               |
| Financiële gegevens                                 |
| Sociale gegevens en gegevens over opleiding, beroep |
| Psychiatrische gegevens                             |
| Gezondheidsgegevens                                 |
| Gegevens verwanten in een dossier                   |

|                                                                    |
|--------------------------------------------------------------------|
| Gegevens derden in een dossier                                     |
| Genetische gegevens                                                |
| Biometrische gegevens                                              |
| Gegevens over fertiliteit en seksualiteit                          |
| Gerechtelijke gegevens                                             |
| Rijksregisternummer                                                |
| Raciale of etnische gegevens, politieke opvattingen, geloof        |
| Gegevens afkomstig van niet medische sensoren (beeld, geluid, ...) |
| GPS-locatiegegevens                                                |
| Toestemmingen en zorgrelaties                                      |
| Verzekerbaarheid                                                   |
| Klachten                                                           |
| <b>Medewerker</b>                                                  |
| Gegevens medewerkers in het EPD                                    |
| Administratieve personeelsgegevens                                 |
| Financiële gegevens                                                |
| Sociale gegevens en gegevens over opleiding, beroep                |
| Gezondheidsgegevens medewerkers                                    |
| Gerechtelijke gegevens                                             |
| Evaluaties en beoordelingen                                        |
| Klachten                                                           |
| Biometrische gegevens                                              |
| Rijksregisternummer                                                |
| <b>Bezoeker/ Andere</b>                                            |
| Administratieve gegevens                                           |
| Financiële gegevens                                                |
| GPS-locatiegegevens                                                |
| Gegevens afkomstig van niet medische sensoren (beeld, geluid, ...) |
| Gegevens afkomstig van online verkeer                              |
| Andere:                                                            |

|                                                                                                   |              |
|---------------------------------------------------------------------------------------------------|--------------|
| De Leverancier,                                                                                   |              |
| Naam en functie van de persoon die tekent namens de Leverancier<br>(wettelijke vertegenwoordiger) |              |
| Datum                                                                                             |              |
| Ik verklaar dat de antwoorden juist zijn en geen belangrijke tekortkomingen verhullen.            | Handtekening |