ADDENDUM BIJ DE LEVERANCIERSOVEREENKOMST M.B.T. GEGEVENSBESCHERMING

Tussen ondergetekende

UZ Brussel, met vestigingseenheidnummer 2.143.464.230, met maatschappelijke zetel te Laarbeeklaan 101, BE-1090 Brussel, deel uitmakend van de rechtspersoon Vrije Universiteit Brussel zoals opgericht bij wet van 28 mei 1970, met maatschappelijke zetel te Pleinlaan 2, BE-1050 Brussel en ondernemingsnummer 0449.012.406, met betrekking tot deze overeenkomst vertegenwoordigd door prof. dr. Mark De Ridder, CEO,

hierna te noemen "**het Ziekenhuis**"

EN

…… [*gegevens leverancier aan te vullen*]

Hierna te noemen "**Leverancier**"

Hierna gezamenlijk aangeduid als de "Partijen"

Overwegende dat

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

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

Het volgende is overeengekomen:

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 inzake Gegevensbescherming en onder de contractuele vrijheid van de Partijen vallen – met opgave van de reden vastgelegd in Annex 1 bij dit Addendum.

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

1. DEFINITIES

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

- **Algemene verordening gegevensbescherming (AVG)**: 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;

- **Gegevensbeschermingswetgeving**: 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, Vewerker, Betrokkene, Toestemming**: de definities zoals bepaald in de Algemene Verordening Gegevensbescherming;

- **Basisovereenkomst**: de overeenkomst tussen het Ziekenhuis en de Leverancier van …… [datum] met betrekking tot …… [volledige titel van de overeenkomst, eventueel referentienummer].

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

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

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

2. TOEPASSINGSGEBIED EN VERHOUDING MET DE BASISOVEREENKOMST

2.1 Dit Addendum vormt een integraal onderdeel van de Basisovereenkomst tussen het Ziekenhuis en de Leverancier. De bepalingen van dit Addendum zijn volledig en onverkort van toepassing op alle verwerkingen van persoonsgegevens die de Leverancier verricht in het kader van de uitvoering van de in Annex 2 gespecificeerde verwerkingsactiviteiten.

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

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 inzake Gegevensbescherming.

3.2 De Leverancier verwerkt de persoonsgegevens uitsluitend op basis van de schriftelijke instructies van het Ziekenhuis, die eenzijdig door het Ziekenhuis worden vastgesteld en zijn opgenomen in **Annex 2** bij dit Addendum. Indien de schriftelijke instructies onduidelijk zijn, stelt de Leverancier het Ziekenhuis hiervan schriftelijk in kennis, waarna de instructies in onderling overleg 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 zonder daarvoor 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.

3.4 Indien Europese of nationale wetgeving de Leverancier verplicht tot een specifieke verwerking, zal de Leverancier het Ziekenhuis voorafgaand aan de verwerking schriftelijk op de hoogte stellen van die wettelijke verplichting, tenzij deze wetgeving een dergelijke kennisgeving verbiedt om gewichtige redenen van algemeen belang.

3.5 Het Ziekenhuis geeft instructies aan de Leverancier in overeenstemming met de Wetgeving inzake Gegevensbescherming en waarborgt dat alle aan de Leverancier toevertrouwde persoonsgegevens op rechtmatige wijze zijn verkregen en kunnen worden verwerkt in het kader van de Basisovereenkomst.

4. PASSENDE TECHNISCHE EN ORGANISATORISCHE MAATREGELEN

4.1 De Partijen nemen passende technische en organisatorische maatregelen om een beveiligingsniveau te waarborgen dat in overeenstemming is met het risico, overeenkomstig artikel 32 van de AVG.

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

4.3 De maatregelen omvatten onder meer, voor zover van toepassing:

- Pseudonimisering en versleuteling van persoonsgegevens;
- De mogelijkheid om de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van verwerkingssystemen en -diensten te waarborgen;
- De mogelijkheid om de beschikbaarheid en toegang tot persoonsgegevens tijdig te herstellen in geval van een fysiek of technisch incident;
- Een proces voor het regelmatig testen, beoordelen en evalueren van de doeltreffendheid van technische en organisatorische maatregelen om de veiligheid van de verwerking te waarborgen.

4.4 Bij het beoordelen van het passende beveiligingsniveau wordt met name rekening gehouden met de verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde openbaarmaking van of toegang tot doorgegeven, opgeslagen of anderszins verwerkte persoonsgegevens, hetzij accidenteel hetzij onrechtmatig.

4.5 De Leverancier houdt zich aan de normen van goedgekeurde gedragscodes en certificeringsmechanismen die binnen de sector van toepassing zijn. Hij levert hiervan het bewijs als Annex bij dit Addendum.

4.6 De Leverancier beschrijft in **Annex 3** de passende technische en organisatorische maatregelen die door hem worden genomen. Hij rapporteert op eigen initiatief aan het Ziekenhuis de wijzigingen in de maatregelen die worden doorgevoerd, zoals uiteengezet in Annex 3, 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 deelt of stelt de persoonsgegevens van het Ziekenhuis alleen ter beschikking aan de vertegenwoordigers, agenten, onderaannemers en werknemers die rechtstreeks betrokken zijn bij de uitvoering van de Basisovereenkomst, op basis van het 'need-to-know'-principe.

De Leverancier waarborgt in het verlengde daarvan dat:

- personen die bevoegd zijn om persoonsgegevens te verwerken, zich ertoe hebben verbonden de vertrouwelijkheid te bewaren of gebonden zijn aan een passende wettelijke geheimhoudingsplicht;
- maatregelen zijn genomen om ervoor te zorgen dat natuurlijke personen die onder zijn gezag handelen en toegang hebben tot de persoonsgegevens, deze gegevens niet verwerken, tenzij op instructie van het Ziekenhuis of op grond van Europese of nationale wetgeving.

.

5.2 De Leverancier mag alleen een derde als subverwerker inschakelen als hij het Ziekenhuis tijdig en in ieder geval vooraf op de hoogte heeft gesteld van de identiteit van de subverwerker en op voorwaarde dat het Ziekenhuis hiertegen geen bezwaar maakt. Indien het Ziekenhuis binnen 14 dagen na ontvangst van de kennisgeving van de Leverancier over de voorgestelde nieuwe subverwerker redelijke bezwaren maakt, zal de Leverancier geen persoonsgegevens van het Ziekenhuis aan de voorgestelde subverwerker bekendmaken, tenzij met de voorafgaande schriftelijke en uitdrukkelijke toestemming van het Ziekenhuis.

5.3 De Leverancier verstrekt het Ziekenhuis de volledige gegevens van de door de subverwerker(s) overgenomen verwerking in **Annex 2** bij dit Addendum.

Indien de Leverancier tijdens de looptijd van de overeenkomst een beroep doet op andere subverwerkers dan die welke aanvankelijk in Annex 2 zijn vermeld, of indien er wijzigingen zijn in de informatie in Annex 2, zal de Leverancier het Ziekenhuis hiervan onmiddellijk op de hoogte stellen. Indien het Ziekenhuis binnen 14 dagen na ontvangst

van de kennisgeving van de Leverancier met betrekking tot de voorgestelde nieuwe subverwerker redelijke bezwaren maakt, zal de Leverancier geen persoonsgegevens van het Ziekenhuis aan de voorgestelde subverwerker verstrekken, tenzij het Ziekenhuis daarvoor voorafgaandelijk uitdrukkelijk schriftelijk toestemming heeft gegeven. In dergelijke gevallen wordt Annex 2 gewijzigd.

Indien de Leverancier een beroep doet op een subverwerker, legt de Leverancier deze subverwerker bij overeenkomst dezelfde verplichtingen inzake gegevensbescherming op als die welke tussen de verwerker en de verwerkingsverantwoordelijke gelden. De Leverancier verstrekt het Ziekenhuis op eerste verzoek de overeenkomst met de subverwerker.

5.4 Indien de subverwerker zijn verplichtingen inzake gegevensbescherming niet nakomt, blijft de Leverancier ten aanzien van het Ziekenhuis volledig aansprakelijk voor de nakoming van de verplichtingen van de subverwerker.

6. OVERDRACHT VAN GEGEVENS NAAR EEN LAND BUITEN DE EUROPESE ECONOMISCHE RUIMTE

6.1 Als persoonsgegevens worden doorgegeven aan een land of organisatie buiten de Europese Economische Ruimte, dient de Leverancier te voldoen aan de waarborgen van hoofdstuk 5 van de AVG en passende waarborgen te bieden. De Leverancier dient het Ziekenhuis voor elke doorgifte buiten de Europese Economische Ruimte te informeren over het volgende:
- het land van de overdracht
- het instrument voor de doorgifte
- de analyse en beoordeling van de aanvullende maatregelen die moeten worden genomen om de overdracht te vergemakkelijken (Transfer Impact Assessment (TIA))

6.2 Wanneer de Leverancier persoonsgegevens verwerkt of laat verwerken buiten de Europese Economische Ruimte, kan het Ziekenhuis de Leverancier verzoeken om de bovengenoemde analyse en beoordeling van de wetgeving en/of toepasselijke praktijken van het derde land, alsmede de aanvullende maatregelen. De Leverancier verstrekt deze beoordeling (Transfer Impact Assessment) op het eerste verzoek van het Ziekenhuis.

6.3 Indien het specifieke overdrachtsinstrument waarnaar wordt verwezen in de artikelen 45 tot en met 49 van de AVG niet doeltreffend is en er geen aanvullende maatregelen worden genomen om het niveau van gegevensbescherming zoals vastgelegd in de AVG te waarborgen, is het de Leverancier niet toegestaan om de persoonsgegevens buiten de Europese Economische Ruimte over te dragen, tenzij het Ziekenhuis hiervoor vooraf schriftelijk toestemming heeft verleend.

6.4 Dit artikel is ook van toepassing op alle overdrachten die worden uitgevoerd door de subverwerkers die door de leverancier zijn ingeschakeld voor de verwerking van persoonsgegevens namens het Ziekenhuis.

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

7.1 Rekening houdend met de aard van de verwerking en de informatie waarover hij beschikt, verbindt de Leverancier zich ertoe het Ziekenhuis bij te staan met betrekking

tot de verantwoordelijkheid van het Ziekenhuis om te voldoen aan de volgende verplichtingen inzake gegevensbescherming:

- Implementatie van passende technische en organisatorische maatregelen om een beveiligingsniveau te waarborgen dat in verhouding staat tot het risico;
- Melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit;
- Mededeling van een inbreuk in verband met persoonsgegevens aan de betrokkene;
- Het uitvoeren van een gegevensbeschermingseffectbeoordeling;
- Raadpleging van de toezichthoudende autoriteit voorafgaand aan de verwerking wanneer uit de gegevensbeschermingseffectbeoordeling blijkt dat de verwerking een hoog risico met zich mee zou brengen indien het ziekenhuis geen maatregelen neemt om het risico te beperken.

7.2 De tijd en middelen die de Leverancier besteedt aan het verlenen van de bijstand zijn voor eigen rekening van de Leverancier.

7.3 Overeenkomstig artikel 7.1 stelt de Leverancier het Ziekenhuis onmiddellijk en gedetailleerd in kennis van een (vermoedelijk) inbreuk op persoonsgegevens en van elk datalek (ook bij de subverwerker) zodra de Leverancier hiervan op de hoogte is. De kennisgeving vindt plaats op een zodanige wijze dat het Ziekenhuis tijdig kan voldoen aan zijn wettelijke verplichtingen als verwerkingsverantwoordelijke op grond van de gegevensbeschermingswetgeving. De Leverancier vrijwaart het Ziekenhuis overeenkomstig artikel 10.2 .

De Leverancier gebruikt voor de melding het meldingsformulier in **Annex 4**.

7.4 De Leverancier verleent ook assistentie bij het onderzoek en de beperking en herstel van een inbreuk op persoonsgegevens. In dit verband verleent hij onder meer assistentie met het oog op de documentatie van maatregelen zoals gegevensbescherming door ontwerp en gegevensbescherming door standaardinstellingen.

7.5 De Leverancier stelt het Ziekenhuis onmiddellijk in kennis van elke klacht, beschuldiging of verzoek (ook indien deze afkomstig is van een toezichthouder) met betrekking tot de verwerking van persoonsgegevens door de Leverancier. De Leverancier biedt alle nodige medewerking en ondersteuning die het Ziekenhuis redelijkerwijs kan verwachten met betrekking tot een dergelijke klacht, beschuldiging of verzoek, onder meer door volledige informatie te verstrekken over een dergelijke klacht, beschuldiging of verzoek, samen met een kopie van de persoonsgegevens van de betrokkene die in het bezit zijn van de Leverancier.

8. VERLENEN VAN BIJSTAND BIJ VERZOEKEN VAN DE BETROKKENEN

8.1 Rekening houdend met de aard van de verwerking, verleent de Leverancier het Ziekenhuis bijstand door middel van passende technische en organisatorische maatregelen bij het nakomen van de verplichting van het Ziekenhuis om te reageren op verzoeken om de rechten van de betrokkene uit te oefenen, zoals gespecificeerd in de Wetgeving inzake Gegevensbescherming.

Dit impliceert onder meer:

- dat de Leverancier alle door het Ziekenhuis gevraagde persoonsgegevens verstrekt binnen de door het Ziekenhuis gevraagde (redelijke) termijn, in ieder geval met inbegrip van de volledige details en kopieën van de klacht, mededeling of verzoek en alle in zijn bezit zijnde persoonsgegevens betreffende de betrokkene;
- dat de Leverancier technische en organisatorische maatregelen neemt die het Ziekenhuis in staat stelt om effectief en tijdig te reageren op relevante klachten, mededelingen of verzoeken.

8.2 De tijd en middelen die de Leverancier besteedt aan het verlenen van de bijstand zijn voor rekening van de leverancier.

8.3 Overeenkomstig artikel 8.1 verbindt de Leverancier zich ertoe het Ziekenhuis onverwijld op de hoogte te stellen indien hij een van de volgende verzoeken ontvangt van een betrokkene (of een derde die namens een betrokkene optreedt):

- een verzoek om toegang tot de verwerkte persoonsgegevens van de betrokkene;
- een verzoek om rectificatie van onjuiste persoonsgegevens;
- een verzoek om verwijdering van persoonsgegevens;
- een verzoek om beperking van de verwerking van persoonsgegevens;
- een verzoek om een draagbare kopie van de persoonsgegevens te verkrijgen of om een kopie aan een derde partij door te geven;
- een bezwaar tegen elke verwerking van persoonsgegevens; of
- elk ander verzoek, elke klacht of mededeling met betrekking tot de verplichtingen van het Ziekenhuis uit hoofde van de wetgeving inzake gegevensbescherming.

8.4 De Leverancier zal niet reageren op verzoeken en aanvragen van de betrokkene zelf, tenzij er schriftelijke afspraken zijn gemaakt tussen het Ziekenhuis en de Leverancier.

9. RECHT VAN CONTROLE DOOR HET ZIEKENHUIS

9.1 Het Ziekenhuis heeft te allen tijde het recht om de naleving van het Addendum door de Leverancier te controleren.

9.2 De Leverancier stelt alle informatie ter beschikking aan het Ziekenhuis die nodig is om aan te tonen dat hij voldoet aan de verplichtingen uit hoofde van de wetgeving inzake gegevensbescherming.

9.3 De Leverancier maakt audits, waaronder inspecties, door het Ziekenhuis of een door het Ziekenhuis gemachtigde auditor mogelijk en werkt hieraan mee. Deze audits kunnen worden aangekondigd of zonder voorafgaande kennisgeving worden uitgevoerd in geval van vermoedelijke onregelmatigheden. De Leverancier verleent volledige medewerking aan een dergelijke audit en levert op verzoek van het Ziekenhuis bewijs van naleving van zijn verplichtingen uit hoofde van dit Addendum.

9.4 De Leverancier stelt het Ziekenhuis onmiddellijk in kennis indien hij van mening is dat een instructie op grond van artikel 9.1 in strijd is met de wetgeving inzake gegevensbescherming.

10. AANSPRAKELIJKHEID

10.1 Partijen zijn elk verantwoordelijk en aansprakelijk voor hun eigen handelingen. De in dit artikel geregelde aansprakelijkheid heeft uitsluitend betrekking op de aansprakelijkheid die voortvloeit uit een schending van de Wetgeving inzake gegevensbescherming en dit Addendum.

10.2 De Leverancier zal het Ziekenhuis schadeloosstellen en vrijwaren voor alle vorderingen, acties, eisen van derden en voor alle schade en verliezen (met inbegrip van boetes opgelegd door de gegevensbeschermingsautoriteit) die direct of indirect voortvloeien uit de verwerking van persoonsgegevens indien hij tijdens de verwerking niet heeft voldaan aan de verplichtingen van de Wetgeving inzake gegevensbescherming die specifiek gericht zijn tot verwerkers, of indien hij buiten of in strijd met de wettige instructies van het Ziekenhuis heeft gehandeld.

10.3 De Partijen zorgen voor een voldoende dekking van hun aansprakelijkheid.

11. EINDE VAN DE OVEREENKOMST

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

11.2 Deze overeenkomst maakt integraal deel uit van de Basisovereenkomst en volgt derhalve het lot van de Basisovereenkomst. Indien de Basisovereenkomst echter wordt beëindigd, blijven de bepalingen van dit Addendum van toepassing voor zover dat nodig is voor de afwikkeling van de verplichtingen in overeenstemming met de Wetgeving inzake gegevensbescherming.

11.3 Onmiddellijk na (ongeacht welke) beëindiging of afloop van de Basisovereenkomst of na afloop van de bewaartermijn zal de Leverancier – naar keuze van het Ziekenhuis – de persoonsgegevens aan het Ziekenhuis retourneren en/of de persoonsgegevens onherroepelijk volledig wissen en bestaande kopieën verwijderen. Indien het Ziekenhuis kiest voor verwijdering van de persoonsgegevens, zal de Leverancier op schriftelijk verzoek aan het Ziekenhuis aantonen dat de verwijdering daadwerkelijk heeft plaatsgevonden.

11.4 De Leverancier kan afwijken van lid 1 indien de opslag van de persoonsgegevens vereist is op grond van Europese of nationale wetgeving.

12. SLOTBEPALINGEN

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

12.2 Dit Addendum is onderworpen aan het Belgische recht. Geschillen worden voorgelegd aan de rechtbanken/hoven in het gerechtelijk arrondissement Brussel (België), die exclusieve territoriale bevoegdheid hebben.

Aldus overeengekomen en opgesteld in tweevoud.

Het Ziekenhuis:	**De Leverancier:**
Prof. Dr. Mark De Ridder CEO **UZ Brussel**	[NAAM] [FUNCTIE]

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: Informatiebeveiliging
Annex 4: Modelformulier melding gegevenslekken
Annex 5: Europese standaardcontractbepalingen (ESCC's) - Optioneel

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

Het Addendum bevat een standaardtekst waarin de verplichtingen uit de wetgeving inzake gegevensbescherming zijn opgenomen. Bepaalde aspecten vallen (binnen bepaalde grenzen) onder de contractuele vrijheid van de partijen.

Indien de partijen bepaalde aspecten anders of specifieker willen regelen of bepaalde zaken willen toevoegen, wordt dit expliciet in deze annex vastgelegd.

Contractuele vrijheid kan bijvoorbeeld betrekking hebben op:

- de termijnen waarbinnen de Leverancier het Ziekenhuis moet informeren of bijstand moet verlenen (maar in elk geval binnen de termijn waarbinnen het Ziekenhuis zelf verslag moet uitbrengen aan de toezichthoudende autoriteit of de betrokken dienst);
- specificatie of specifieke of algemene toestemming van toepassing is voor de subverwerker(s);
- …

Wijzigingen in deze Annex zijn enkel geldig en afdwingbaar indien deze Annex door beide partijen is ondertekend en gedateerd.

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

Aldus overeengekomen en in tweevoud opgesteld te …….. op …….. .

Het Ziekenhuis:	**De Leverancier:**
Prof. dr. Mark De Ridder	[NAAM]
CEO	[FUNCTIE]
UZ Brussel	

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

Begeleidende nota

Deze Annex beschrijft de specifieke verwerkingen door de Leverancier, waarvoor het Ziekenhuis instructies geeft bij het sluiten van de Basisovereenkomst of bij het ondertekenen 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 Basisovereenkomst inzake …… *[aan te vullen door leverancier]*.

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

……
……
……

II. De categorieën van persoonsgegevens die het Ziekenhuis de Leverancier opdraagt te verwerken (aanduiden wat van toepassing is en indien nodig aanvullen):

- contactgegevens
- financiële gegevens
- factuurgegevens
- loongegevens
- medische gegevens
- marketinggegevens
- gegevens over het gebruik door het Ziekenhuis van de diensten en aanverwante producten van de Leverancier
- overige (te specificeren):
  ……
  ……
  ……

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

- patiënten van het Ziekenhuis

- vertrouwenspersonen, vertegenwoordigers en contactpersonen van de patiënten van het Ziekenhuis
- verzorgers 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 waar nodig aanpassen/aanvullen):

Het Ziekenhuis geeft hierbij de volgende instructies voor de verwerking van persoonsgegevens (onverminderd de instructies die rechtstreeks voortvloeien uit de bepalingen van de Basisovereenkomst of dit Addendum of die redelijkerwijs nodig zijn om de Leverancier in staat te stellen zijn verplichtingen correct na te komen):

- Raadpleging van persoonsgegevens
  Dit betreft diensten die door de Leverancier worden geleverd waarbij persoonsgegevens van het Ziekenhuis kunnen worden ingezien door medewerkers of onderaannemers van de Leverancier, waaronder, maar niet beperkt tot, servicedesk diensten, (remote) monitoring diensten, systeembeheer diensten, technisch applicatiebeheer/management, vulnerability scanning diensten, rapporting diensten op het gebied van governance en software asset management diensten, het leveren van support (helpdesk, remote monitoring, etc.).

- Opslag van persoonsgegevens
  Dit betreft diensten die door de Leverancier worden geleverd waarbij persoonsgegevens van het Ziekenhuis worden opgeslagen in een door de Leverancier geleverd opslagsysteem, zoals, maar niet beperkt tot, cloudopslagdiensten, cloud back-up diensten, file diensten, directory diensten, managed file transfer, e-mail & calendaring en logbestandsverwerking, het bieden van ondersteuning (helpdesk, monitoring op afstand, enz.).

- Overdracht van persoonsgegevens
  Dit verwijst naar diensten die door de Leverancier worden geleverd waarbij persoonsgegevens van het Ziekenhuis worden verzonden door, naar of tussen applicaties op een door de Leverancier beheerd platform, met inbegrip van, maar niet beperkt tot, LAN-diensten, Wide Area Network-diensten, datacenterinterconnectiviteitsdiensten, loadbalancing, SAN-switchinterconnecties en diensten die worden geleverd met behulp van Voice over Internet Protocol (VoIP).

- Aanpassing of wijziging van persoonsgegevens
  Dit verwijst naar diensten die door de Leverancier worden geleverd en waarbij persoonsgegevens van het Ziekenhuis handmatig of automatisch kunnen worden aangepast, bijvoorbeeld in een geautomatiseerde workflow die wordt ondersteund door een job scheduling system.

- Software testen
  Dit verwijst naar diensten die door de Leverancier worden geleverd waarbij databases van het

Ziekenhuis die persoonsgegevens bevatten (persoonsgegevens die niet zijn geanonimiseerd) buiten de productieomgeving (in test, acceptatie, enz.) worden gebruikt als onderdeel van het testproces van de softwareapplicatie van het Ziekenhuis.

- [In te vullen - optioneel]

IV. De bewaartermijnen van de (verschillende categorieën) persoonsgegevens:

De Leverancier bewaart de verwerkte persoonsgegevens op een passende, veilige manier gedurende de periode die nodig is om de schriftelijke instructies van het Ziekenhuis uit te voeren, en met betrekking tot de onderstaande categorieën persoonsgegevens, gedurende de hieronder gespecificeerde periode **[invullen indien de opslagperiode in maanden kan worden uitgedrukt]**:

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

V. De functionaris voor gegevensbescherming of andere verantwoordelijke contactpersonen voor gegevensbescherming en -verwerking:

Voor het Ziekenhuis
Contactgegevens: gegevensbescherming@uzbrussel.be en/ofdpo@vub.be .

Voor de Leverancier (vul aan)
Naam:
Contactgegevens:

VI. Lijst van subverwerkers

Afhankelijk van de overeengekomen raamovereenkomst(en) zal de verwerker voor zijn dienstverlening gebruikmaken van enkele of alle van de volgende subverwerkers en locaties. *Gelieve de lijst te vervolledigen met alle subverwerkers, inclusief apps, SaaS-platforms, online accounts, cloudproviders, softwareplug-ins, op cookies gebaseerde uitwisselingen, enz.*

naam subverwerker	*Adres maatschappelijke zetel*	*Plaats (locatie) van de verwerking*	*Aard van de verwerking (beschrijving van de aard van de verwerking, assets, enz.)*

VII. Lijst van doorgiften/transfers naar derde landen

Gegevensexporteur	*Gegevensimporteur*	*Land waar de persoonsgegevens worden verwerkt*	*Overdrachtsinstrument (SCC, BCR, ...) en aanvullende maatregelen (indien noodzakelijk) (*)*

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

ANNEX 3 – INFORMATIEBEVEILIGING

Vragenlijst informatiebeveiliging en gegevensbescherming voor de verwerker

Naam van de organisatie (derde partij)	Naam: ..... Adres: .... Ondernemingsnummer (Kruispuntbank): .....
Voornaam, achternaam en e-mailadres van de Chief Information Security Officer (CISO) (verplicht)	....
Voornaam, achternaam en e-mailadres van de contactpersoon voor informatiebeveiliging (assistent-CISO) (optioneel)	....
Voornaam, achternaam en e-mailadres van de functionaris voor gegevensbescherming (DPO) (verplicht)	....
Voornaam, achternaam en e-mailadres van de lokale contactpersoon voor gegevensbescherming (assistent-DPO of vertegenwoordiger) (optioneel)	....
Voornaam, achternaam en e-mailadres van de persoon die verantwoordelijk is voor het dagelijks beheer (CEO, verplicht)	....

Vraag	*Plaats een kruisje (X) in het vakje dat overeenkomt met uw antwoord*		Geef uitleg in geval van een 'nee'-antwoord
1	Heeft u een formeel, actueel informatiebeveiligingsbeleid dat is goedgekeurd door de persoon die verantwoordelijk is voor het dagelijks beheer?	☐ JA ☐ NEE	
2	Heeft u een risicobeoordeling voor elk proces/project voor informatiebeveiliging/gegevensbescherming dat u gebruikt voor het leveren van diensten?	☐ JA ☐ NEE	
3	Binnen uw organisatie: • is er een afdeling die verantwoordelijk is voor informatiebeveiliging en die rechtstreeks rapporteert aan de persoon die verantwoordelijk is voor het dagelijks beheer van de organisatie?	☐ JA ☐ NEE ☐ JA ☐ NEE	
4	Heeft u een informatiebeveiligingsplan dat is goedgekeurd door de persoon die verantwoordelijk is voor het dagelijks beheer?	☐ JA ☐ NEE	
5	Hoeveel uur werken de CISO en zijn/haar team? • CISO • Team Hoeveel uur training op het gebied van informatiebeveiliging hebben de DPO en zijn/haar team gevolgd? • DPO • Team	1) uren/maand 2) uur/maand 3) uren/jaar 4) uren/jaar	
6	Heeft u procedures voor de ontwikkeling van nieuwe systemen of ingrijpende wijzigingen in bestaande systemen, zodat de projectleider rekening kan houden met de beveiligingsvereisten die in de minimale beveiligingsnormen zijn beschreven?	JA ☐ NEE ☐ N.v.t. ☐	
7	Neemt u passende maatregelen zodat de professionele, vertrouwelijke en gevoelige gegevens die op mobiele media zijn opgeslagen, alleen toegankelijk zijn voor bevoegde personen?	☐ JA ☐ NEE	
8	Neemt u, afhankelijk van het toegangsmedium, passende maatregelen voor de informatiebeveiliging van de toegang van buiten uw organisatie tot de professionele, vertrouwelijke en gevoelige gegevens?	☐ JA ☐ NEE	

Vraag	*Plaats een kruisje (X) in het vakje dat overeenkomt met uw antwoord*		Geef uitleg in geval van een 'nee'-antwoord
9	Beschikt u over telewerkfaciliteiten die zodanig zijn ingericht dat op de telewerkplek (thuis, in een satellietkantoor of op een andere locatie) geen informatie zonder versleuteling op externe apparaten wordt opgeslagen en dat mogelijke bedreigingen vanaf de telewerkplek de IT-infrastructuur niet kunnen	☐ JA ☐ NEE	
10	Wijst u elk jaar alle medewerkers op informatiebeveiliging en gegevensbescherming en voert u jaarlijks een evaluatie uit van de naleving van dit beleid in de praktijk?	☐ JA ☐ NEE	
11	Heeft u de toegang beveiligd door middel van een duidelijke toegangsprocedure en heeft u een (logisch of fysiek) toegangssysteem geïmplementeerd om ongeoorloofde toegang te voorkomen?	☐ JA ☐ NEE	
12	Heeft u een classificatiesysteem voor persoonsgegevens waarvoor u de diensten verleent en past u dit classificatiesysteem toe?	☐ JA ☐ NEE	
13	Heeft u de regels, zoals gespecificeerd in een beleidslijn inzake 'E-mail, online communicatie en internetgebruik', verwerkt in een informatiebeveiligingsbeleid?	☐ JA ☐ NEE	
14	Heeft u ten minste één toegangsbeheerder aangesteld wanneer u gebruikmaakt van externe toegang tot de zorginstelling?	☐ JA ☐ NEE	
15	Heeft u uw personeel aangemoedigd om de extra veiligheidsmaatregelen die de zorgverlening oplegt (indien van toepassing) te lezen en toe te passen?	☐ JA ☐ NEE	
16	Als u 'cryptografie' wilt toepassen: • heeft u een formeel beleid voor het gebruik van cryptografische controles? • heeft u een formeel beleid voor het gebruik, de bescherming en de levensduur van cryptografische sleutels voor de gehele levenscyclus?	☐ JA ☐ NEE ☐ JA ☐ NEE	
17	Neemt u de nodige maatregelen om de toegang tot de gebouwen en terreinen te beperken tot bevoegde personen en controleert u deze toegang zowel tijdens als buiten de werkuren?	☐ JA ☐ NEE	
18	Neemt u de nodige maatregelen om verlies, beschadiging, diefstal of compromittering van apparatuur en onderbreking van de activiteiten te voorkomen?	☐ JA ☐ NEE	
19	In het geval van hergebruik van de informatiedrager, gebruikt u deze dan opnieuw op een gegevensclassificatieniveau dat ten minste vergelijkbaar is?	☐ JA ☐ NEE	

Vraag	*Plaats een kruisje (X) in het vakje dat overeenkomt met uw antwoord*		Geef uitleg in geval van een 'nee'-antwoord
20	Heeft u contractueel met de opdrachtgever passende maatregelen voor het wissen van gegevens vastgelegd?	☐ JA ☐ NEE	
21	Past u de regels met betrekking tot het loggen van toegang toe zoals bepaald door de opdrachtgever?	☐ JA ☐ NEE	
22	Zijn er regels vastgesteld voor de aanschaf, ontwikkeling en het onderhoud van systemen tussen de verschillende betrokken partijen?	☐ JA ☐ NEE	
23	Werken alle medewerkers met ICT-middelen voor de uitvoering van hun taken op basis van minimale autorisatie voor de uitvoering van hun taak?	☐ JA ☐ NEE	
24	Zijn de toegangsbeveiligingsvereisten (identificatie, authenticatie, autorisatie) gedefinieerd, gedocumenteerd, gevalideerd en gecommuniceerd? Worden deze toegangen geregistreerd?	☐ JA ☐ NEE ☐ JA ☐ NEE	
25	Zijn de risico's op het gebied van beveiliging en gegevensbescherming contractueel vastgelegd tussen u en eventuele onderaannemers?	☐ JA ☐ NEE	
26	Gebruikt u een checklist zodat de projectleider de zekerheid kan krijgen dat alle beleidslijnen inzake informatiebeveiliging en gegevensbescherming correct zijn geëvalueerd en indien nodig zijn geïmplementeerd tijdens de ontwikkelingsfase van het project?	☐ JA ☐ NEE	
27	Controleert u telkens wanneer een project in productie wordt genomen of de beveiligings- en gegevensbeschermingsvereisten die aan het begin van het project zijn vastgesteld, ook daadwerkelijk zijn geïmplementeerd?	☐ JA ☐ NEE	
28	Zijn er onder toezicht van de projectleider gescheiden faciliteiten voor ontwikkeling, testen en/of acceptatie en productie, inclusief de daarmee samenhangende scheiding van verantwoordelijkheden binnen het project?	☐ JA ☐ NEE	
29	Wordt elke toegang tot persoonlijke en vertrouwelijke gegevens geregistreerd in overeenstemming met een registratiebeleid en de toepasselijke wet- en regelgeving?	☐ JA ☐ NEE	
30	Is in de projectspecificaties opgenomen hoe de toegang tot en het gebruik van systemen en applicaties worden geregistreerd om bij te dragen aan het opsporen van afwijkingen met betrekking tot informatiebeveiliging en gegevensbescherming?	☐ JA ☐ NEE	

Vraag	*Plaats een kruisje (X) in het vakje dat overeenkomt met uw antwoord*		Geef uitleg in geval van een 'nee'-antwoord
31	Voldoet het logboekbeheer ten minste aan de volgende doelstellingen? • De informatie om te kunnen bepalen door wie, wanneer en hoe toegang is verkregen tot welke informatie • De identificatie van de aard van de geraadpleegde informatie • De duidelijke identificatie van de persoon	☐ JA ☐ NEE	
32	Zijn de nodige hulpmiddelen beschikbaar gesteld om de loggegevens door de bevoegde personen te laten verwerken?	☐ JA ☐ NEE	
33	Komen de transactionele/functionele loggegevens overeen met de bewaartermijn die geldt voor de gegevens zelf (bijvoorbeeld 30 jaar voor medische gegevens)?	☐ JA ☐ NEE	
34	Zijn de projectresultaten (verwerkte gegevens, documentatie (broncode, programma's, technische documenten, enz.) geïntegreerd in het back-upbeheersysteem?	☐ JA ☐ NEE	
35	Zijn tijdens de ontwikkeling van het project de vereisten met betrekking tot de continuïteit van de dienstverlening geformaliseerd, in overeenstemming met uw verwachtingen?	☐ JA ☐ NEE	
36	Zijn uw continuïteitsplan en de bijbehorende procedures bijgewerkt in overeenstemming met de ontwikkeling van het project, inclusief	☐ JA ☐ NEE	
37	Wordt er aan het begin van het project een risicoanalyse uitgevoerd om de noodprocedures vast te stellen?	☐ JA ☐ NEE	
38	Worden de procedures voor incidentbeheer tijdens de ontwikkeling van het project geformaliseerd en gevalideerd?	☐ JA ☐ NEE	
39	Wordt de CISO op de hoogte gebracht van beveiligingsincidenten en de DPO van incidenten met betrekking tot gegevensbescherming?	☐ JA ☐ NEE	
40	Wordt de documentatie (technisch, procedures, handleidingen, enz.) tijdens de levenscyclus van het project up-to-date gehouden?	☐ JA ☐ NEE	
41	Wordt alle apparatuur, inclusief aangeschafte of ontwikkelde systemen, toegevoegd aan de inventaris van de operationele middelen?	☐ JA ☐ NEE	
42	Wordt er passende medewerking verleend aan audits in de vorm van het ter beschikking stellen van personeel, documentatie, logboekbeheer en andere redelijkerwijs beschikbare informatie?	☐ JA ☐ NEE	
43	Zijn de vereisten met betrekking tot informatiebeveiliging en gegevensbescherming gedocumenteerd om de risico's met betrekking tot de toegang tot informatietools te beperken?	☐ JA ☐ NEE	
45	Zijn alle relevante vereisten met betrekking tot informatiebeveiliging en privacy opgesteld en overeengekomen tussen u en derden/leveranciers (die	☐ JA ☐ NEE	

Vraag	*Plaats een kruisje (X) in het vakje dat overeenkomt met uw antwoord*		Leg uit in het geval van een 'nee'-antwoord
	informatie van de organisatie lezen, verwerken, opslaan, communiceren of ICT-infrastructuurcomponenten en ICT-diensten leveren)?		
46	Worden de diensten die door derden/leveranciers aan u worden geleverd, gecontroleerd, geëvalueerd en geauditeerd?	☐ JA ☐ NEE	
47	Worden de veranderingen in de dienstverlening aan u door de derde partij/leverancier beheerd, inclusief het bijhouden van gegevens over bestaande beleidslijnen, procedures/maatregelen voor informatiebeveiliging en	☐ JA ☐ NEE	
48	Heeft u een beleid voor cloud computing wanneer u gebruikmaakt van clouddiensten?	☐ JA ☐ NEE	
49	Wanneer u professionele, vertrouwelijke of gevoelige gegevens in een cloud wilt verwerken, voldoet u dan aan de minimale contractuele garanties?	☐ JA ☐ NEE	
50	Heeft u procedures voor het vaststellen en beheren van incidenten met betrekking tot informatiebeveiliging of gegevensbescherming, met de bijbehorende verantwoordelijkheden, en heeft u deze procedures intern bekendgemaakt?	☐ JA ☐ EE	
51	Heeft u een overeenkomst met alle medewerkers waarin staat dat elke medewerker (vast of tijdelijk, intern of extern) verplicht is om ongeoorloofde toegang, gebruik, wijziging, openbaarmaking, verlies of vernietiging van informatie en informatiesystemen te melden?	☐ JA ☐	
52	Worden incidenten en zwakke punten op het gebied van informatiebeveiliging of gegevensbescherming met betrekking tot informatie en informatiesystemen aan de opdrachtgever gemeld, zodat u en de opdrachtgever tijdig passende corrigerende maatregelen kunnen nemen?	☐ JA ☐ EE	
53	Heeft de leverancier een procedure om incidenten met betrekking tot informatiebeveiliging/gegevensbescherming zo snel mogelijk intern te communiceren/melden?	☐ JA ☐ NEE	
54	Wordt bij incidenten op het gebied van informatiebeveiliging of gegevensbescherming het bewijsmateriaal correct verzameld in overeenstemming met de wettelijke en reglementaire vereisten?	☐ JA ☐ NEE	
55	Wordt elk incident op het gebied van informatiebeveiliging of gegevensbescherming formeel gevalideerd, zodat procedures en controlemaatregelen kunnen worden verbeterd, en worden de lessen die uit een incident zijn getrokken, gecommuniceerd aan uw management voor validatie en	☐ JA ☐ NEE	

Vraag	*Plaats een kruisje (X) in het vakje dat overeenkomt met uw antwoord*		Leg uit in het geval van een 'nee'-antwoord
56	Heeft u een continuïteitsplan voor alle kritieke processen en essentiële informatiesystemen?	☐ JA ☐ NEE	
57	Zijn informatiebeveiliging en gegevensbescherming een integraal onderdeel van uw continuïteitsbeheer?	☐ JA ☐ NEE	
58	Heeft u een eigen continuïteitsplan? Wordt dit plan regelmatig getest en aangepast, met de nodige communicatie naar uw management voor validatie en goedkeuring?	☐ JA ☐ NEE ☐ JA ☐ NEE	
59	Voert u periodiek een conformiteitsaudit uit met betrekking tot de situatie op het gebied van informatiebeveiliging en gegevensbescherming?	☐ JA ☐ NEE	
60	Heeft u een formele disciplinaire procedure voor werknemers die de informatiebeveiliging en gegevensbescherming hebben geschonden?	☐ JA ☐ NEE	
61	Verzamelt u regelmatig alle informatie om de risico's in verband met de naleving van de AVG in kaart te brengen en neemt u de nodige maatregelen als gevolg van een hoog 'residueel' risico van niet-naleving?	☐ JA ☐ NEE	
62	Heeft u een actueel centraal register van de verwerkingsverantwoordelijke of de verwerker en bent u formeel verantwoordelijk voor het niet-implementeren van controlemaatregelen die gericht zijn op naleving van de Europese verordening voor de specifieke verwerking?	☐ JA ☐ NEE	

Datum en handtekening van de CISO of functionaris voor gegevensbescherming (DPO) van de organisatie (derde partij) (optioneel)	..... Datum Handtekening
Datum en handtekening van de persoon die verantwoordelijk is voor het dagelijks beheer van de organisatie (derde partij) **(verplicht)**	..... Datum Handtekening

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

ANNEX 4 – MODELFORMULIER MELDING GEGEVENSLEKKEN

Contactgegevens van de contactpersoon van het ziekenhuis (24/7 bereikbaar):
Afdeling/dienst:
Telefoonnummer

Datum:
Bedrijfsnaam:
Adres:
Postcode:
BTW-nummer
Wie heeft de inbreuk ontdekt?
Naam:
Functie:
Wanneer werd de inbreuk ontdekt?
Datum:
Tijd:
Beschrijf het beveiligingsincident waarbij de inbreuk op de beveiliging van persoonsgegevens plaatsvond:

Wanneer vond de inbreuk plaats?
a. Op (datum + tijd)
b. Tussen (datum + tijd) en (datum + tijd)
c. Nog niet vastgesteld
d. Er is een anonieme melding gedaan door een derde partij
Stel de context vast van de gegevens die bij de inbreuk betrokken zijn:
Classificatie van de gegevens:
a. Geen, de gegevens kunnen niet aan een individu worden gekoppeld
b. Naam- en adresgegevens
c. Telefoonnummers
d. E-mailadressen, Facebook-ID's, Twitter-ID's, enz.
e. Gebruikersnamen, wachtwoorden of andere inloggegevens, klantnummers
f. Financiële gegevens: rekeningnummers, creditcardnummers
g. Nationaal registratienummer
h. Kopieën van identiteitsdocumenten
i. Geslacht, geboortedatum en/of leeftijd
j. Gegevens over iemands religie of levensbeschouwing, ras, politieke overtuiging of lidmaatschap van een vakbond
k. Gegevens over iemands gezondheid of seksuele geaardheid
l. Persoonsgegevens op grond van het strafrecht of persoonsgegevens over onwettig of hinderlijk gedrag in verband met een verbod dat als gevolg van dat gedrag is opgelegd
m. Gegevens over iemands financiële of economische situatie, gegevens over schulden, salaris en betalingsgegevens
n. Afgeleide financiële gegevens (inkomenscategorie, eigenwoningbezit, autobezit)
o. Levensstijlkenmerken (waaronder gezinssamenstelling, woonsituatie, interesses, demografische kenmerken (leeftijd, geslacht, nationaliteit, beroep, opleiding)
p. Gegevens verkregen uit (openbare) sociale profielen (Facebook-, LinkedIn- en Twitter-accounts, enz.)
q. Overige, namelijk:

Classificatie van de context van de inbreuk:

Om **hoeveel** personen gaat het bij de inbreuk?

a. Geen, de gegevens kunnen niet aan een individu worden toegeschreven

b. Nog niet vastgesteld

c. Ten minste …… (aantal), maar niet meer dan ……..(aantal) betrokken

Beschrijf de groep personen van wie de persoonsgegevens bij de inbreuk betrokken waren:

Omstandigheden van het datalek:

a. Alleen-lezen (een onbevoegde derde partij heeft (vertrouwelijke) gegevens kunnen inzien. De verwerker heeft de gegevens nog steeds in zijn bezit.) – **Vertrouwelijkheid is in gevaar**

b. Kopiëren (een onbevoegde derde partij heeft gegevens kunnen kopiëren. De gegevens zijn nog steeds in het bezit van de verwerker.) – **Vertrouwelijkheid is in gevaar**

c. Wijziging (een onbevoegde derde partij heeft gegevens in de systemen van de verwerker kunnen wijzigen – **Integriteit is in gevaar**

d. Verwijdering of vernietiging (een onbevoegde derde partij heeft gegevens uit de systemen van de verwerker verwijderd of vernietigd) – **Beschikbaarheid is in gevaar**

e. Diefstal – **Beschikbaarheid is in gevaar**

f. Nog niet bekend

Waren de persoonsgegevens onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegde derden, bijvoorbeeld door middel van versleuteling en hashing?

Ja

Nee

Gedeeltelijk, d.w.z.

Zo ja, hoe werden de persoonsgegevens versleuteld?
Waren er personen uit andere EU-lidstaten bij de inbreuk betrokken?
Ja
Nee
Zo ja, welke EU-lidstaten:
Welke beveiligingsmaatregelen (technisch en organisatorisch) zijn genomen om de inbreuk aan te pakken en verdere inbreuken te voorkomen?
Met wie kan contact worden opgenomen voor meer informatie over de inbreuk?
Naam van de contactpersoon van de Leverancier:
E-mail:
Telefoonnummer:

ANNEX 5 – EUROPESE STANDAARDCONTRACTBEPALINGEN (ESCC'S) – OPTIONEEL

[TOE TE VOEGEN]