**OVEREENKOMST VERWERKING PERSOONSGEGEVENS**

**BIJLAGE BIJ DE BASISOVEREENKOMST d.d. xxx**

**Tussen**

UZ Leuven

met zetel te Herestraat 49, 3000 Leuven

rechtsgeldig vertegenwoordigd door haar gedelegeerd bestuurder

Hierna genoemd **‘de Opdrachtgever’**

**En**

**‘de Opdrachtnemer’**

Hierna gezamenlijk genoemd **‘de Partijen’**

**Overwegende dat**

* De Opdrachtnemer leveringen en/of diensten zal verrichten ten behoeve van de Opdrachtgever, zoals beschreven in de Basisovereenkomst, waardoor deze persoonsgegevens zal verwerken en de Partijen met deze Bijlage afspraken wensen vast te leggen over deze verwerking van persoonsgegevens;
* De Opdrachtnemer een expert is in de leveringen en/of diensten die het voorwerp zijn van de Basisovereenkomst, de Opdrachtnemer beschikt over de nodige middelen om de leveringen en/of diensten te volbrengen volgens de regels van de kunst en kon dit aantonen middels relevante en betrouwbare referenties;

**wordt overeengekomen als volgt**

# Begrippenkader

## Voor de toepassing van deze Bijlage gelden de volgende begripsomschrijvingen:

### **Algemene Verordening Gegevensbescherming (GDPR)**: Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG, met haar wijzigingen en Europese uitvoeringswetgeving;

### **Wetgeving Gegevensbescherming**: de Algemene Verordening Gegevensbescherming, andere Europese regelgeving waarin bepalingen met betrekking tot gegevensbescherming en privacy worden opgenomen, evenals de toepasselijke nationale wetgeving inzake gegevensbescherming en privacy in de lidstaten met haar wijzigingen en uitvoeringsbesluiten, met inbegrip van voor de sector toepasselijke goedgekeurde gedragscodes;

### **Persoonsgegevens, verwerking, verwerkingsverantwoordelijke, verwerker, betrokkene, toestemming**: de begripsomschrijvingen zoals bepaald in de Algemene Verordening Gegevensbescherming;

### **Basisovereenkomst**: de overeenkomst tussen de Opdrachtgever en de Opdrachtnemer voor uitvoering van werken, levering van diensten of producten, waarvan huidige verwerkingsovereenkomst de bijlage van uitmaakt.

## De Opdrachtnemer levert leveringen en/of diensten aan de Opdrachtgever op grond van en zoals gedefinieerd in de Basisovereenkomst. Voor de verwerkingsactiviteiten zoals bepaald in **Annex 1** bij deze Bijlage geldt volgende kwalificatie:

## de Opdrachtgever bepaalt het doel en minstens de essentiële middelen van de verwerking en is bijgevolg verwerkingsverantwoordelijke;

## de Opdrachtnemer verricht de verwerking van persoonsgegevens ten behoeve van en volgens de instructies van de Opdrachtgever en is bijgevolg verwerker.

# Toepassingsgebied en verhouding met de basisovereenkomst

## Deze Bijlage maakt integraal deel uit van de Basisovereenkomst gesloten tussen de Opdrachtgever en de Opdrachtnemer. De bepalingen uit deze Bijlage zijn onverkort van toepassing op alle verwerkingen van persoonsgegevens die de Opdrachtnemer verricht in het kader van de uitvoering van de verwerkingsactiviteiten bepaald in **Annex 1**.

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

## Alle kosten die de Opdrachtnemer dient te doen om te voldoen aan de vereisten zoals vermeld in deze Bijlage worden geacht begrepen te zijn in de prijs die werd opgegeven in de Basisovereenkomst.

# Verwerking conform de regelgeving en de schriftelijke instructies van de Opdrachtgever

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

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

## Behoudens andersluidende bepalingen in deze Bijlage, zal de Opdrachtnemer 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 Economische Ruimte zonder daartoe een schriftelijke instructie te hebben ontvangen van de Opdrachtgever. Een verwerking conform de instructies van de Opdrachtgever kan ook betekenen dat de verwerking (onmiddellijk) moet worden stopgezet.

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

## De Opdrachtgever geeft instructies aan de Opdrachtnemer in overeenstemming met de Wetgeving Gegevensbescherming en waarborgt dat alle persoonsgegevens die aan de Opdrachtnemer worden toevertrouwd rechtmatig werden verkregen en kunnen worden verwerkt in het kader van de Basisovereenkomst.

## De Opdrachtnemer stelt de Opdrachtgever onmiddellijk in kennis indien naar zijn mening een instructie een inbreuk oplevert op de Wetgeving Gegevensbescherming.

# Passende technische en organisatorische maatregelen

## De Partijen treffen passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen in overeenstemming met artikel 32 GDPR.

## 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:

## Pseudonimisering en versleuteling van persoonsgegevens;

## Het vermogen om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen en diensten te garanderen;

## Het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te herstellen;

## Een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

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

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

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

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

Enkel voor de opdrachten waarin de Opdrachtgever zelf voor beperkte periode aan de Opdrachtnemer toegang geeft tot bepaalde persoonsgegevens en deze verwerking gebeurt in het bijzijn/onder toezicht van een aangestelde van de Opdrachtgever (bijvoorbeeld in het kader van opdrachten IT-support bij onderhoud of incident,…) vervalt de verplichting van de Opdrachtnemer om certificatie voor te leggen. Alle andere instructies zoals beschreven in **Annex 2**, alsook de verbintenissen in het kader van confidentialiteit zoals beschreven in **Annex 3** blijven in dergelijk geval evenwel van toepassing.

# Verwerking door een ‘Subverwerker’ of werknemer

## De Opdrachtnemer waarborgt dat de bepalingen van deze Bijlage worden nageleefd door zijn vertegenwoordigers, agenten, onderaannemers en werknemers. De Opdrachtnemer zal persoonsgegevens van de Opdrachtgever enkel delen met of beschikbaar maken voor de vertegenwoordigers, agenten, onderaannemers en werknemers die rechtstreeks betrokken zijn bij de uitvoering van de Basisovereenkomst op basis van het ‘need-to-know’-principe.

##

## De Opdrachtnemer waarborgt in het verlengde daarvan dat:

## de tot het verwerken van persoonsgegevens gemachtigde personen zich er contractueel toe hebben verbonden om de vertrouwelijkheid in acht te nemen dan wel door een passende wettelijke verplichting van vertrouwelijkheid zijn gebonden;

## dat er maatregelen zijn getroffen om ervoor te zorgen dat iedere natuurlijke persoon die handelt onder diens gezag en toegang heeft tot de persoonsgegevens, deze slechts in opdracht van de Opdrachtgever verwerkt, tenzij hij door Europese of nationale regelgeving tot verwerking is gehouden.

## De Opdrachtnemer maakt bij de ondertekening van deze Bijlage in **Annex 1** elk van de Subverwerkers waarop beroep wordt gedaan kenbaar en de Opdrachtgever verleent door ondertekening hiervoor algemene toestemming. De Opdrachtnemer zal elke nieuwe Subverwerker aan de Opdrachtgever mede delen middels **Annex 5**. De Opdrachtgever houdt zich het recht voor om zich te allen tijde te verzetten tegen één of meerdere Subverwerkers. Indien de Opdrachtgever binnen 14 dagen na ontvangst van de melding van de Opdrachtnemer enig bezwaar (op redelijke gronden) uit met betrekking tot de voorgestelde nieuwe Subverwerker, zal de Opdrachtnemer geen persoonsgegevens van de Opdrachtgever doorgeven aan de voorgestelde Subverwerker, tenzij met voorafgaande schriftelijke en expliciete toestemming van de Opdrachtgever.

## Indien de Opdrachtnemer een Subverwerker inschakelt, zal hij een schriftelijke overeenkomst aangaan met deze Subverwerker waarin dezelfde of gelijkwaardige verplichtingen opgenomen worden als deze van de Opdrachtnemer zoals uiteengezet in deze Bijlage en in overeenstemming met artikel 28 GDPR. Wanneer de Subverwerker zijn verplichtingen inzake gegevensbescherming niet nakomt, blijft de Opdrachtnemer volledig aansprakelijk ten aanzien van de Opdrachtgever voor het nakomen van de verplichtingen van de Subverwerker.

# Verlenen van bijstand bij de verplichtingen m.b.t. het gegevensbeschermingsbeleid van de Opdrachtgever

## Rekening houdend met de aard van de verwerking en de hem ter beschikking staande informatie, verbindt de Opdrachtnemer zich ertoe bijstand te verlenen aan de Opdrachtgever in de verantwoordelijkheid van de Opdrachtgever 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 door de Opdrachtgever van een inbreuk in verband met persoonsgegevens aan de toezichthoudende overheid;

## de mededeling door de Opdrachtgever van een inbreuk in verband met persoonsgegevens van de betrokkene aan de betrokkene;

## het uitvoeren van een gegevensbeschermingseffectbeoordeling;

## het voorafgaand raadplegen door de Opdrachtgever van de toezichthoudende overheid indien uit de gegevensbeschermingseffectbeoordeling blijkt dat de verwerking een hoog risico zou opleveren indien de Opdrachtgever geen maatregelen neemt om het risico te beperken.

## De tijd en middelen die de Opdrachtnemer spendeert voor het verlenen van de bijstand zijn voor eigen rekening van de Opdrachtnemer.

## In het verlengde van Artikel 6.1, licht de Opdrachtnemer de Opdrachtgever omstandig en onmiddellijk in over een (vermoedelijke) inbreuk in verband met persoonsgegevens (ook bij de Subverwerker) zodra de Opdrachtnemer hiervan kennis heeft genomen. De kennisgeving gebeurt op een dergelijke wijze dat de Opdrachtgever tijdig kan voldoen aan haar wettelijke verplichtingen als verwerkingsverantwoordelijke onder de Wetgeving Gegevensbescherming. De Opdrachtnemer vrijwaart de Opdrachtgever conform Artikel 10.2.

## Voor de melding gebruikt de Opdrachtnemer het meldingsformulier in **Annex 4**. De Opdrachtnemer 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.

## De Opdrachtnemer stelt de Opdrachtgever onmiddellijk in kennis van enige gemaakte klacht, beschuldiging of aanvraag (ook indien afkomstig van een regulator) met betrekking tot de verwerking van persoonsgegevens voor de Opdrachtgever. De Opdrachtnemer biedt alle nodige medewerking en ondersteuning die de Opdrachtgever 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 Opdrachtnemer.

# Doorgiften buiten de Europese Economische ruimte

## Indien persoonsgegevens worden doorgegeven naar een land of organisatie buiten de Europese Economische Ruimte, zal de Opdrachtnemer de waarborgen van hoofdstuk 5 GDPR naleven en passende waarborgen voorzien.

## De Opdrachtnemer zal bij elke doorgifte buiten de Europese Economische Ruimte de Opdrachtgever informeren over:

## Het land van de doorgifte

## Het doorgifte-instrument

## De analyse en beoordeling betreffende de aanvullende maatregelen die moeten worden genomen om de doorgifte door te voeren.

## Wanneer de Opdrachtnemer de persoonsgegevens buiten de Europese Economische Ruimte zal (laten) verwerken kan de Opdrachtgever deze beoordeling van het recht en/of de geldende praktijken van het derde land opvragen bij de Opdrachtnemer (Transfer Impact Assessment).

## Indien het concrete doorgifte-instrument van art. 45 tot en met 49 GDPR niet doeltreffend is en er geen aanvullende maatregelen worden genomen om het niveau van gegevensbescherming te vrijwaren, zoals vastgelegd in de GDPR, is het de Opdrachtnemer niet toegelaten om de persoonsgegevens door te geven buiten de Europese Economische ruimte, behoudens wanneer de Opdrachtgever voorafgaandelijk zijn schriftelijke toestemming hiervoor heeft verleend.

## Dit artikel heeft tevens betrekking op eventuele doorgiftes die gebeuren door de Subverwerkers die de Opdrachtnemer hanteert voor de verwerking van persoonsgegevens in opdracht van de Opdrachtgever.

# Verlenen van bijstand bij verzoeken van de betrokkenen

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

##

## Dit impliceert onder meer:

* + dat de Opdrachtnemer alle door de Opdrachtgever opgevraagde persoonsgegevens bezorgt, binnen de door de Opdrachtgever 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 Opdrachtnemer zulke technische en organisatorische maatregelen implementeert die de Opdrachtgever toelaten doeltreffend en tijdig te antwoorden op relevante klachten, mededelingen of aanvragen.

De tijd en middelen die de Opdrachtnemer spendeert voor het verlenen van de bijstand zijn voor eigen rekening van de Opdrachtnemer.

## In het verlengde van Artikel 8.1, verbindt de Opdrachtnemer zich ertoe de Opdrachtgever 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 de Opdrachtgever onder de Wetgeving Gegevensbescherming.

De Opdrachtnemer beantwoordt de verzoeken en aanvragen van de betrokkenen niet zelf, behoudens eventuele andersluidende schriftelijke afspraken tussen de Opdrachtgever en de Opdrachtnemer.

# Recht op controle door de Opdrachtgever

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

# Aansprakelijkheid

## De 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 Bijlage.

## De Opdrachtnemer vergoedt en vrijwaart de Opdrachtgever 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 de Opdrachtgever is gehandeld.

## De Partijen zorgen voor een afdoende dekking van hun aansprakelijkheid.

# Einde van de overeenkomst

## Indien de Opdrachtnemer de verplichtingen uit deze Bijlage niet correct vervult en nalaat passende maatregelen te treffen binnen een termijn van maximaal twee maanden, kan de Opdrachtgever – onverminderd andere beëindigingsgronden zoals voorzien in de Basisovereenkomst – de Basisovereenkomst na voormelde termijn van twee maanden onmiddellijk verbreken en/of de verwerkingsopdracht stopzetten.

## Deze Bijlage 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 Bijlage evenwel gelden voor zover nodig voor de afwikkeling van de verplichtingen conform de Wetgeving Gegevensbescherming.

## Onmiddellijk bij (eender welke) beëindiging of verstrijken van de Basisovereenkomst, dan wel na afloop van de bewaartermijn, zal de Opdrachtnemer – naar keuze van de Opdrachtgever – de persoonsgegevens terugbezorgen aan de Opdrachtgever en/of de persoonsgegevens volledig en onherroepelijk wissen, en bestaande kopieën verwijderen. In het geval de Opdrachtgever kiest voor het verwijderen van de persoonsgegevens, zal de Opdrachtnemer op schriftelijk verzoek van de Opdrachtgever aantonen dat de verwijdering daadwerkelijk gebeurd is.

## De Opdrachtnemer kan van het eerste lid afwijken indien de opslag van de persoonsgegevens door Europese of nationale wetgeving verplicht is en de Opdrachtnemer de Opdrachtgever over deze verplichting in kennis heeft gesteld.

# Slotbepalingen

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

## Deze Bijlage wordt beheerst door het Belgisch recht. Geschillen worden voorgelegd aan de rechtbanken/hoven in het gerechtelijk arrondissement Leuven, die exclusieve territoriale bevoegdheid hebben.

\* \*

\*

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

**De Opdrachtgever** **De** **Opdrachtnemer**

***Annexen***

Annex 1: De verwerkingsopdracht en -instructies zoals bepaald door de Opdrachtgever

Annex 2: Overige instructies voor de verwerking van persoonsgegevens en minimale veiligheidsmaatregelen

Annex 3: Verbintenissen in het kader van confidentialiteit

Annex 4: Modelformulier voor melding van gegevenslekken

Annex 5: Modelformulier voor aanpassingen aan Annex I na afsluiten verwerkingsovereenkomst

**Annex 1**

**De verwerkingsopdracht en -instructies zoals bepaald door de Opdrachtgever**

***Inleidende opmerking***

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

1. **Het doel van de verwerking van persoonsgegevens**

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

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

1. **De categorieën van persoonsgegevens die de Opdrachtgever laat verwerken door de Opdrachtnemer (aanduiden wat van toepassing is en zo nodig aanvullen):**
* contactgegevens
* financiële gegevens
* factuurgegevens
* loongegevens
* gegevens over gezondheid
* marketing gegevens
* gegevens over het gebruik door de Opdrachtgever van de diensten en bijhorende producten van de Opdrachtnemer
* andere (te specificeren):

…………………………………………………………………………………………………

1. **De categorieën van betrokkenen van wie de persoonsgegevens verwerkt worden (aanduiden wat van toepassing is en zo nodig aanvullen):**
* patiënten van de Opdrachtgever
* vertrouwenspersonen, vertegenwoordigers en contactpersonen van de patiënten van de Opdrachtgever
* zorgverleners van de patiënten van de Opdrachtgever
* personeelsleden van de Opdrachtgever
* andere (te specificeren):

…………………………………………………………………………………………………

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

De Opdrachtgever geeft hierbij de volgende instructies tot verwerking van de persoonsgegevens (onverminderd de instructies die rechtstreeks voortvloeien uit de bepalingen van de Basisovereenkomst of de Bijlage of die redelijkerwijze vereist zijn voor de juiste uitvoering door de Opdrachtnemer van zijn verplichtingen):

* Persoonsgegevens raadplegen
* Persoonsgegevens opslaan
* Persoonsgegevens doorzenden
* Persoonsgegevens bijwerken of wijzigen
* Software testen
* Leveren van support
* Andere: …………………………………..

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

1. **De bewaartermijnen van de (verschillende categorieën) persoonsgegevens:**

De Opdrachtnemer bewaart de verwerkte persoonsgegevens op adequaat beveiligde wijze gedurende de periode die nodig is voor het uitvoeren van de schriftelijke instructies van de Opdrachtgever en volgens de bepalingen zoals overeengekomen in de Basisovereenkomst.

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

1. **Lijst van Subverwerkers die voor de Opdrachtnemer persoonsgegevens verwerken ten behoeve van de uitvoering van de Basisovereenkomst tussen Opdrachtgever en Opdrachtnemer (gelieve in volgende tabel te specifiëren):**

|  |  |  |
| --- | --- | --- |
| **Naam Subverwerker** | **Adres** | **Diensten die worden uitgevoerd door de Subverwerker** |
|  |  |  |
|  |  |  |
|  |  |  |

1. **Lijst van doorgiftes/transfers van persoonsgegevens buiten de Europese Economische Ruimte, inclusief transfers van Subverwerkers (gelieve in volgende tabel te specifiëren):**

|  |  |  |  |
| --- | --- | --- | --- |
| **Gegevensexporteur** | **Gegevensimporteur** | **Land waar de persoonsgegevens worden verwerkt** | **Doorgifte-instrument & aanvullende maatregelen (indien noodzakelijk)** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

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

**Voor de Opdrachtgever**

Naam: DPO UZ LEUVEN – 016 33 22 11

 Contactgegevens: GDPR@UZLeuven.be

 **Voor de Opdrachtnemer**

Naam:

 Contactgegevens:

**Annex 2**

**Overige instructies voor de verwerking van persoonsgegevens en minimale veiligheidsmaatregelen**

1. De Opdrachtgever vereist dat bij de verwerking van persoonsgegevens te allen tijde conform de ISO/IEC 27001 en 27002 Standaarden gehandeld wordt. De Opdrachtnemer legt bij voorkeur certificatie voor deze normen voor. Indien de Opdrachtnemer niet over ISO/IEC 27001 en 27002 certificatie beschikt, kan de Opdrachtgever andere gelijkwaardige certificaten aanvaarden, maar dient de Opdrachtnemer steeds minstens volgens de geest van de ISO/IEC 27001 en 27002 Standaarden te werken.
2. De Opdrachtnemer bevestigt daarnaast om minimaal de hierna volgende technische en organisatorische maatregelen te nemen, onverminderd de instructies die rechtstreeks voortvloeien uit de bepalingen van de Basisovereenkomst of de Bijlage of die redelijkerwijze vereist zijn voor de juiste uitvoering door de Opdrachtnemer van zijn verplichtingen.

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

**Minimale maatregelen voor Opdrachtnemers en hun Subverwerkers:**

**1. Persoonsgegevens raadplegen binnen en buiten UZ Leuven**

Voor de verwerkingen waarbij persoonsgegevens UZ Leuven niet verlaten gelden cumulatief de volgende minimum maatregelen:

* 1. De persoonsgegevens kunnen enkel door het eigen personeel van de Opdrachtnemer worden geraadpleegd en dit in zoverre strikt noodzakelijk voor het uitvoeren van de opdracht zoals omschreven in de Basisovereenkomst.
	2. De Opdrachtnemer bezorgt op eenvoudige vraag van de Opdrachtgever een actuele lijst van de personen die voor de uitoefening van hun opdracht noodzakelijk toegang nodig hebben tot de systemen. Hierin wordt tevens de reden van de aanvraag van toegangsrechten gemotiveerd. Wijzigingen in deze lijst worden door de Opdrachtnemer onmiddellijk gecommuniceerd aan de Opdrachtgever.
	3. Elk van de personen die toegang krijgt wordt door de Opdrachtnemer onderworpen aan de vertrouwelijkheids- en discretieplicht zoals opgesteld door de Opdrachtgever (zie **Annex 3**).
	4. Elk van de personen die toegang krijgt tot gevoelige gegevens bij de Opdrachtgever wordt door de Opdrachtnemer voldoende opgeleid en geïnformeerd over verplichtingen en verantwoordelijkheden bij het (potentieel) raadplegen van persoonsgegevens. De Opdrachtgever kan bijkomend eisen dat een opleiding zoals ter beschikking gesteld door de Opdrachtgever gevolgd wordt.
1. **Persoonsgegevens opslaan buiten UZ Leuven**

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

* 1. Door in te schrijven verklaart de Opdrachtnemer over de volgende documenten te beschikken. De Opdrachtnemer zal deze aan de Opdrachtgever overhandigen op eenvoudig verzoek.
		1. De geïmplementeerde Information Security Policy (ISP) samen met de bevestiging dat de policy door de hoogste hiërarchie en diverse verantwoordelijken werd goedgekeurd.

In de ISP wordt minstens beschreven:

* + - * hoe confidentialiteit, integriteit en veiligheid verzekerd worden bij in- en output, in transit en at-rest;
			* hoe om wordt gegaan met versleuteling van gegevens (encryptie, pseudonimisering, codering), of deze standaard wordt toegepast aan de kant van de Opdrachtnemer en wie hiervoor verantwoordelijk is binnen de Opdrachtnemer;
			* hoe de verantwoordelijkheden en de ingestelde organisatorische regels intern verdeeld werden;
			* het Security Information and Event Management Plan dat veiligheidsincidenten en data logs analyseert; en
			* daar waar wettelijk vereist, de contactgegevens van de informatieveiligheidsconsulent en/of DPO.
		1. Het geïmplementeerd Back-up and Disaster Recovery Plan dat minstens specifieert:
			- welke back-up mechanismes worden gebruikt en of deze afdoende zijn;
			- welke recovery testen worden gebruikt en of de rapportering hiervan beschikbaar is.
		2. De geïmplementeerde Identity and Access Management (IAM) policy die ten minste de volgende principes ondersteunt:
			- duidelijk gedefinieerde, rolgebaseerde toegangsrechten;
			- intrekken van toegang bij einde samenwerking;
			- strong Authentication;
			- full logging van IAM en data access.
		3. De geïmplementeerde Incident Management Procedure. Deze beschrijft minstens hoe gevolgen van incidenten voor de data van de Opdrachtgever beperkt worden, welke de te nemen stappen zijn bij ontdekking van een veiligheidsincident en welke personen verantwoordelijk zijn om het incident aan te pakken en zo een gezonde toestand te herstellen.
	1. De Opdrachtnemer bevestigt te voldoen aan de volgende technische en organisatorische vereisten:
		1. De gegevens verkregen van of via de Opdrachtgever mogen de grenzen van de Europese Economische Ruimte niet verlaten. Indien zij deze grenzen toch verlaten, dient de Opdrachtnemer de nodige garanties voor te leggen die bewijzen dat de doorgifte voldoet aan Hoofdstuk V van de Algemene Verordening Gegevensbescherming (Doorgifte van persoonsgegevens aan derde landen of internationale organisaties).
		2. De netwerken waarover gegevens worden verstuurd (vast of draadloos, van, naar of tussen applicaties, of via een door de Opdrachtnemer 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)) beveiligd te hebben volgens het defense-in-depth principe en voor de verzending van gevoelige gegevens aangepaste technieken te gebruiken.
		3. De hardware (inclusief VM) uitgerust te hebben met afdoende toezichtmechanismes en beveiligingssystemen om data lekken te voorkomen en te analyseren.
		4. De gebruikte informaticasystemen overeenkomstig hun classificatie te hebben geplaatst in geïdentificeerde en beschermde lokalen waartoe de toegang beperkt is.
		5. Alle server stations te hebben uitgerust met preventie en detectie mechanismen, alsook middelen om virussen en andere malware in te dijken en de server stations dienen een hardening process te hebben ondergaan.
		6. Alle server stations te hebben uitgerust met een patch management proces (geïmplementeerd en gedocumenteerd).
		7. Voor alle server stations patches te testen in een acceptance omgeving vooraleer deze uit te rollen.
		8. De systemen minimum 1x per jaar aan een penetration test en/of ethical hacking te onderwerpen, bij voorkeur in samenwerking met de Opdrachtgever.
	2. De Opdrachtnemer garandeert de implementatie van deze maatregelen te kunnen staven door middel van externe rapportering, opgemaakt met een minimum van 1x per 3 jaar en dit volgens een nauwkeurig omschreven stramien. Bij de inschrijving voegt de Opdrachtnemer de laatste externe rapportering toe of een document dat aangeeft door wie, wanneer en volgens welke basis de rapportering werd opgemaakt.
	3. De Opdrachtnemer kan nooit overgaan tot aanpassing van de persoonsgegevens van de Opdrachtgever - hetzij op manuele dan wel op geautomatiseerde wijze - buiten voor deze gevallen waarvoor expliciete toestemming bestaat van de Opdrachtgever.
	4. De Opdrachtnemer garandeert dat bij (eender welke) beëindiging of verstrijken van de Basisovereenkomst, dan wel na afloop van de bewaartermijn, op vraag en naar keuze van de Opdrachtgever, alle data veilig vernietigd worden en dit voor alle media die gebruikt worden voor gegevensopslag.
1. **Gebruik van Cloud Storage Diensten voor de opslag van gegevens buiten UZ Leuven**

In geval het om Cloud Storage Diensten gaat, vereist de Opdrachtgever bijkomend aan de bovenstaande maatregelen en cumulatief dat de Opdrachtnemer voldoet aan volgende voorwaarden:

* 1. Er gebruik wordt gemaakt van een private cloud oplossing of, in een multi-tenant systeem, de data van de Opdrachtgever technisch gesegregeerd of geïsoleerd worden.
	2. De Opdrachtnemer de reversibility van het opslagsysteem en dat van de Subverwerkers kan verzekeren.
	3. De uitvoering en management van de opslagsystemen geregeld is in SLA’s (Service Level Agreements).
	4. De Opdrachtnemer een business continuity plan kan voorleggen op eenvoudige vraag van de Opdrachtgever.
	5. De Opdrachtnemer in zijn Back-up en Retention Plan specifieert aan welke Recovery Time Objective en Recovery Point Objective kan voldaan worden door de Cloud Service.

1. vertrouwelijk / aangetekend / drukwerk

2. aanspreektitel voornaam naam

3. functie en/of afdeling

4. firma of organisatie

5. straat en nummer of postbusnummer

6. postcode en gemeente

7. land

**Annex 3**

**Verbintenissen in het kader van confidentialiteit**

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

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

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

Indien in het kader van de opdracht toegang verleend wordt tot elektronische systemen van UZ Leuven, in bijzonder het KWS (Klinisch Werkstation), zal de Opdrachtnemer of zijn/haar aangestelde zich steeds volledig schikken naar alle binnen UZ Leuven geldende reglementen, voorschriften en procedures betreffende het gebruik van deze systemen.

Dit houdt o.a. in dat

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

**Annex 4**

**Modelformulier voor melding van gegevenslekken**

|  |
| --- |
| Gegevens contactpersoon van de Opdrachtgever (bereikbaar 24/7): |
| Dienst: DPO  |
| Telefoonnummer: 016 33 22 11 – email: gdpr@uzleuven.be  |

|  |
| --- |
| Datum: |
|  |
| Bedrijfsnaam: |
| Adres: |
| Postcode: |
| BTW-nummer: |
|  |
| Wie heeft de inbreuk geconstateerd? |
| Naam: |
| Functietitel: |
|  |
| Wanneer is de inbreuk geconstateerd? |
| Datum: |
| Tijd: |
|  |
| Omschrijf het beveiligingsincident waarbij de inbreuk op de beveiliging van persoonsgegevens zich heeft voorgedaan: |
| Wanneer heeft de inbreuk plaatsgevonden? |
| 1. Op (datum + tijd)
 |
| 1. Tussen (datum + tijd) en (datum + tijd)
 |
| 1. Is nog niet vastgesteld
 |
| 1. Er is sprake van een anonieme melding door een derde
 |
|  |
| Vastleggen context van de data betrokken bij de inbreuk:  |
| Classificatie van de data: |
| 1. Geen, de gegevens zijn niet herleidbaar tot een individu
 |
| 1. Naam, adres en woonplaats gegevens
 |
| 1. Telefoonnummers
 |
| 1. E-mailadressen, Facebook ID’s, Twitter ID’s etc.
 |
| 1. Gebruikersnamen, wachtwoorden of andere inloggegevens, klantnummers
 |
| 1. Financiële gegevens: rekeningnummers, creditcardnummers
 |
| 1. Rijksregisternummer
 |
| 1. Kopieën van identiteitsbewijzen
 |
| 1. Geslacht, geboortedatum, en/of leeftijd
 |
| 1. Gegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid of lidmaatschap van een vakvereniging
 |
| 1. Gegevens over iemands gezondheid of seksuele geaardheid
 |
| 1. Strafrechtelijke persoonsgegevens of persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag
 |
| 1. Gegevens over iemands financiële of economische situatie, gegevens over schulden, salaris- en betalingsgegevens
 |
| 1. Afgeleide financiële data (inkomenscategorie, huizenbezit, autobezit)
 |
| 1. Lifestyle kenmerken (o.a. gezinssamenstelling, woonsituatie, interesses), demografische kenmerken (leeftijd, geslacht, nationaliteit, beroep, onderwijs)
 |
| 1. Data verkregen uit (openbare) sociale profielen (Facebook-, LinkedIn- en Twitteraccounts, …)
 |
| 1. Overig, namelijk:
 |
|  |
| Classificatie van de context betrokken bij de inbreuk: |
| Van hoeveel personen zijn persoonsgegevens betrokken bij de inbreuk? |
| 1. Geen, de gegevens zijn niet herleidbaar tot een individu
 |
| 1. Nog niet bepaald
 |
| 1. Ten minste …………………………………… (aantal), maar niet meer dan …………………………..(aantal) betrokkenen
 |
| Omschrijf de groep mensen waarvan persoonsgegevens zijn betrokken bij de inbreuk: |
|  |
| Omstandigheden van het gegevenslek: |
| 1. Alleen lezen (een niet geautoriseerde derde heeft (vertrouwelijke) data kunnen inzien. Verwerker heeft de data nog in zijn bezit.) - Confidentialiteit is in gevaar
 |
| 1. Kopiëren (een niet-geautoriseerde derde heeft data kunnen kopiëren. De data is ook nog in het bezit van Verwerker.) - Confidentialiteit is in gevaar
 |
| 1. Wijzigen (een niet-geautoriseerde derde heeft data gewijzigd, of kunnen wijzigen, in systemen van Verwerker) - Integriteit is in gevaar
 |
| 1. Verwijderen of vernietigen (een niet-geautoriseerde derde heeft data verwijderd uit de systemen van Verwerker of data vernietigd.) - Beschikbaarheid is in gevaar
 |
| 1. Diefstal - Beschikbaarheid is in gevaar
 |
| 1. Nog niet gekend
 |
|  |
| Zijn de persoonsgegevens onbegrijpelijk of ontoegankelijk gemaakt voor ongeautoriseerde derden, bijvoorbeeld door encryptie en hashing? |
| Ja |
| Nee |
| Deels, namelijk |
|  |
| Zo ja, op welke manier zijn de persoonsgegevens versleuteld: |
|  |
| Heeft de inbreuk betrekking op personen uit andere EU-landen? |
| Ja |
| Nee |
| Zo ja, welke EU-landen: |
|  |
| Welke beveiligingsmaatregelen (technisch en organisatorisch) zijn getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen? |
|  |
| Wie kan benaderd worden voor meer informatie over de inbreuk? |
| Naam contactpersoon van de Opdrachtnemer: |
| E-mail: |
| Telefoonnummer: |

**Annex 5**

**Modelformulier voor aanpassingen aan Annex 1 na afsluiten verwerkingsovereenkomst**

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

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

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

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

**De Opdrachtgever** **De** **Opdrachtnemer**