**ADDENDUM LEVERANCIERSOVEREENKOMST M.B.T. GEGEVENSBESCHERMING**

**Tussen ondergetekenden**

[Ziekenhuis] waarvan de maatschappelijke zetel gevestigd is te ………………………………………………………………………., rechtsgeldig vertegenwoordigd door *[aan te vullen door betreffende dienst]*

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 met zich brengen dat persoonsgegevens worden verwerkt en de partijen met dit Addendum de afspraken wensen vast te leggen over de verwerking van persoonsgegevens in het kader van de diensten

**wordt overeengekomen als volgt:**

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

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

# Begrippenkader

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

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

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

### **Persoonsgegevens, Verwerking, Verwerkingsverantwoordelijke, Verwerker, Betrokkene, Toestemming**: de begripsomschrijvingen zoals bepaald in de Algemene Verordening Gegevensbescherming;

### **Basisovereenkomst**: de overeenkomst tussen het Ziekenhuis en de Leverancier van ……………………………. [datum] met betrekking tot …………………………………………………………………………………………………………[invullen titel overeenkomst, evt. referentienummer].

## 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 de middelen van de verwerking en is bijgevolg verwerkingsverantwoordelijke;

## de Leverancier verricht de verwerking van persoonsgegevens ten behoeve van het Ziekenhuis als verwerkingsverantwoordelijke en is bijgevolg verwerker.

# Toepassingsgebied en verhouding met de basisovereenkomst

## 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 verwerkingen van persoonsgegevens die de Leverancier verricht in het kader van de uitvoering van de verwerkingsactiviteiten bepaald in Annex 2.

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

# Verwerking conform de regelgeving en de schriftelijke instructies van het ziekenhuis

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

## De Leverancier verwerkt de persoonsgegevens uitsluitend op basis van de schriftelijke instructies van het Ziekenhuis, eenzijdig bepaald door het Ziekenhuis en zoals opgenomen in **Annex 2** bij dit Addendum. Indien de schriftelijke instructies niet duidelijk zijn, meldt de leverancier dit schriftelijk aan het Ziekenhuis waarop in onderling overleg de instructies worden verduidelijkt.

## Behoudens andersluidende bepalingen in dit Addendum zal de Leverancier de persoonsgegevens niet voor eigen doeleinden of die van derden verwerken, noch de persoonsgegevens aan derden verstrekken, noch deze doorsturen naar een land gelegen buiten de Europese Unie zonder daartoe een schriftelijke instructie te hebben ontvangen van het Ziekenhuis. Een verwerking conform de instructies van het Ziekenhuis kan ook betekenen dat de verwerking (onmiddellijk) moet worden stopgezet.

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

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

# Passende technische en organisatorische maatregelen

## De Partijen treffen passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen.

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

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

# Verwerking door een “Subverwerker” of werknemer

## De Leverancier waarborgt dat de bepalingen van dit Addendum worden nageleefd door zijn vertegenwoordigers, agenten, onderaannemers en werknemers.

## De Leverancier waarborgt in het verlengde daarvan dat:

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

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

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

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

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

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

## Wanneer de subverwerker zijn verplichtingen inzake gegevensbescherming niet nakomt, blijft de Leverancier volledig aansprakelijk ten aanzien van het Ziekenhuis voor het nakomen van de verplichtingen van de subverwerker.

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

## Rekening houdend met de aard van de verwerking en de hem ter beschikking staande informatie, verbindt de Leverancier zich ertoe bijstand te verlenen aan het Ziekenhuis in de verantwoordelijkheid van het Ziekenhuis om volgende verplichtingen in het kader van gegevensbescherming na te leven:

## het treffen van passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen;

## het melden van een inbreuk in verband met persoonsgegevens aan de toezichthoudende overheid;

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

## het uitvoeren van een gegevensbeschermingseffectbeoordeling;

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

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

## In het verlengde van artikel 6.1, licht de Leverancier het Ziekenhuis omstandig en onmiddellijk in over een (vermoedelijke) inbreuk in verband met persoonsgegevens alsook over iedere gegevenslek (ook bij de subverwerker) zodra de Leverancier hiervan kennis heeft genomen. De kennisgeving gebeurt op een dergelijke wijze dat het Ziekenhuis tijdig kan voldoen aan haar wettelijke verplichtingen als verwerkingsverantwoordelijke onder de Wetgeving Gegevensbescherming. De Leverancier vrijwaart het Ziekenhuis conform artikel 9.2.

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

De Leverancier levert tevens bijstand in het onderzoek naar en de beperking en remediëring van een inbreuk in verband met een verwerking van persoonsgegevens. Daarbij zal hij onder meer ook bijstand verlenen met het oog op het documenteren van maatregelen zoals gegevensbescherming door ontwerp en door standaardinstellingen.

## De Leverancier stelt het Ziekenhuis onmiddellijk in kennis van enige gemaakte klacht, beschuldiging of aanvraag (ook indien afkomstig van een regulator) met betrekking tot de verwerking van persoonsgegevens door de Leverancier. De Leverancier biedt alle nodige medewerking en ondersteuning die het Ziekenhuis redelijkerwijze kan verwachten met betrekking tot dergelijke klacht, beschuldiging of aanvraag, onder meer door volledige informatie te verstrekken over dergelijke klacht, beschuldiging of aanvraag samen met een kopie van de persoonsgegevens betreffende de betrokkene in het bezit van de Leverancier.

# Verlenen van bijstand bij de verzoeken van de betrokkenen

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

## Dit impliceert onder meer:

* + dat de Leverancier alle door het Ziekenhuis opgevraagde persoonsgegevens bezorgt, binnen de door het Ziekenhuis verzochte (redelijke) tijdsspanne, in ieder geval met inbegrip van de volledige details en kopieën van de klacht, mededeling of aanvraag en enige persoonsgegevens in zijn bezit met betrekking tot een betrokkene;
  + dat de Leverancier zulke technische en organisatorische maatregelen implementeert die het Ziekenhuis toelaten doeltreffend en tijdig te antwoorden op relevante klachten, mededelingen of aanvragen.

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

## In het verlengde van artikel 7.1 verbindt de Leverancier zich ertoe het Ziekenhuis onverwijld in te lichten indien hij van een betrokkene (of derde handelend voor rekening van een betrokkene) een van de volgende verzoeken krijgt:

## een aanvraag tot inzage tot de persoonsgegevens die van de betrokkene worden verwerkt;

## een aanvraag tot rectificatie van onjuiste persoonsgegevens;

## een aanvraag tot wissing van persoonsgegevens;

## een aanvraag tot beperking van de verwerking van persoonsgegevens;

## een aanvraag tot het verkrijgen van een draagbare kopie van de persoonsgegevens, of tot overdracht van een kopie aan een derde;

## een bezwaar tegen enige verwerking van persoonsgegevens; of

## elke andere aanvraag, klacht of mededeling met betrekking tot de verplichtingen van het Ziekenhuis onder de Wetgeving Gegevensbescherming.

De Leverancier beantwoordt de verzoeken en aanvragen van de betrokkenen niet zelf, behoudens eventuele andersluidende schriftelijke afspraken tussen het Ziekenhuis en de Leverancier.

# Recht op controle door het ziekenhuis

## Het Ziekenhuis heeft steeds het recht om de naleving door de Leverancier van het Addendum te controleren.

## De Leverancier stelt het Ziekenhuis alle informatie ter beschikking die nodig is om de nakoming van de verplichtingen in het kader van de Wetgeving Gegevensbescherming aan te tonen.

## De Leverancier maakt audits, waaronder inspecties, door het Ziekenhuis of een door het Ziekenhuis gemachtigde controleur, mogelijk en draagt er aan bij. De Leverancier verleent volledige medewerking met betrekking tot een dergelijke audit en levert, op vraag van het Ziekenhuis, het bewijs van de naleving van zijn verplichtingen onder dit Addendum.

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

# Aansprakelijkheid

## Partijen zijn ieder verantwoordelijk en aansprakelijk voor hun eigen handelen. De in dit artikel geregelde aansprakelijkheid heeft uitsluitend betrekking op de aansprakelijkheid ten gevolge van een inbreuk op de Wetgeving Gegevensbescherming en op dit Addendum.

## De Leverancier vergoedt en vrijwaart het Ziekenhuis voor alle claims, acties, aanspraken van derden en voor alle schade en verliezen (waaronder ook boetes van de Gegevensbeschermingsautoriteit) die rechtstreeks of onrechtstreeks voortvloeien uit een verwerking van persoonsgegevens wanneer bij de verwerking niet is voldaan aan de specifiek tot de verwerkers gerichte verplichtingen van de Wetgeving Gegevensbescherming of wanneer buiten dan wel in strijd met de rechtmatige instructies van het Ziekenhuis is gehandeld.

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

# Einde van de overeenkomst

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

## Deze overeenkomst vormt een geheel met de Basisovereenkomst en volgt dan ook het lot van de Basisovereenkomst. Ingeval de Basisovereenkomst een einde neemt, blijven de bepalingen van dit Addendum 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 Leverancier – naar keuze van het Ziekenhuis – de persoonsgegevens terugbezorgen aan het Ziekenhuis en/of de persoonsgegevens volledig en onherroepelijk wissen, en bestaande kopieën verwijderen. In het geval het Ziekenhuis kiest voor het verwijderen van de persoonsgegevens, zal de Leverancier op schriftelijk verzoek van het Ziekenhuis aantonen dat de verwijdering daadwerkelijk gebeurd is.

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

# Slotbepalingen

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

## Dit Addendum wordt beheerst door het Belgisch recht. Geschillen worden voorgelegd aan de rechtbanken/hoven in het gerechtelijk arrondissement Antwerpen, afdeling Antwerpen, die exclusieve territoriale bevoegdheid hebben.

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

[Naam] [Naam]

**[Het Ziekenhuis]** **Leverancier**

**Annexen**

Annex 1: aanpassingen aan het addendum bij contractuele vrijheid van de partijen

Annex 2: de verwerkingsopdracht en -instructies zoals bepaald door het ziekenhuis

Annex 3: de informatiebeveiliging

Annex 4: modelformulier melding gegevenslekken

**Annex 1 – Aanpassingen aan het Addendum bij contractuele vrijheid van de partijen**

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

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

Tot de contractuele vrijheid kunnen bijvoorbeeld behoren:

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

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

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

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

[Naam] [Naam]

**[Het Ziekenhuis]** **Leverancier**

**Annex 2 - De verwerkingsopdracht- en instructies zoals bepaald door het ziekenhuis**

***Begeleidende nota***

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

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

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

De verwerking van Persoonsgegevens door de Leverancier gebeurt in het kader van de uitvoering van de 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 laat verwerken door de Leverancier (aanduiden wat van toepassing is en zo nodig aanvullen) :**

* contactgegevens
* financiële gegevens
* factuurgegevens
* loongegevens
* medische gegevens
* marketing gegevens
* gegevens over het gebruik door het Ziekenhuis van de diensten en bijhorende producten van de Leverancier
* andere (te specificeren) :

…………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………….

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

* patiënten van het Ziekenhuis
* vertrouwenspersonen, vertegenwoordigers en contactpersonen van de patiënten van het Ziekenhuis
* zorgverleners van de patiënten van het Ziekenhuis
* personeelsleden van het Ziekenhuis
* andere (te specificeren):

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………….

**IV. De verwerking van de persoonsgegevens (aanduiden wat van toepassing is en aanpassen/aanvullen waar nodig) :**

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

* Persoonsgegevens raadplegen

Het gaat om diensten van de Leverancier waarbij de persoonsgegevens van het Ziekenhuis bekeken kunnen worden door medewerkers of Onderaannemers van de Leverancier, waaronder maar niet beperkt tot, servicedesk Diensten, (remote) monitoring Diensten, system management Diensten, technisch applicatie management, vulnerability scanning Diensten, rapporting Diensten in governance en software asset management Diensten

* Persoonsgegevens opslag

Het gaat om diensten van de Leverancier waarbij de persoonsgegevens van het Ziekenhuis opgeslagen worden in een door de Leverancier geleverd opslagsysteem zoals onder meer maar niet beperkt tot cloud storage Diensten, cloud backup Diensten, file Diensten, directory Diensten, managed file transfer, mail & calendaring and logfile processing.

* Persoonsgegevens doorzenden

Het betreft diensten van de Leverancier waarbij persoonsgegevens van het Ziekenhuis verzonden worden van, naar of tussen applicaties op een door de Leverancier beheerd platform zoals onder meer maar niet beperkt tot LAN Diensten, Wide Area Network Diensten, data center interconnectiviteitsdiensten, Loadbalancing, SAN switch interconnects en Diensten die geleverd worden over de Voice over Internet Protocol (VoIP).

* Persoonsgegevens bijwerken of wijzigen

Het betreft diensten van de Leverancier waarbij persoonsgegevens van het Ziekenhuis aangepast kunnen worden zowel op manuele, als op geautomatiseerde wijze zoals bij een geautomatiseerde job flow die ondersteund wordt door een job scheduling system.

* Software testen

Het gaat om diensten van de Leverancier waarbij databanken van het Ziekenhuis die persoonsgegevens bevatten (persoonsgegevens die niet geanonimiseerd zijn), worden gebruikt buiten de productie omgeving (in test, acceptatie,…) als onderdeel van het testproces van de Ziekenhuis software applicatie.

* XXX
* XXX
* XXX
* XXX
* [Aan te vullen]

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

De Leverancier bewaart de verwerkte persoonsgegevens op adequaat beveiligde wijze gedurende de periode die nodig is voor het uitvoeren van de schriftelijke instructies van het Ziekenhuis, en voor wat de onderstaande categorieën persoonsgegevens betreft gedurende de hierna bepaalde periode **[aanvullen indien bewaartermijn kan worden uitgedrukt in maanden]** :

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

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

**Voor het Ziekenhuis**

Naam:

Contactgegevens:

**Voor de Leverancier**

Naam:

Contactgegevens:

**Annex 3 – De informatiebeveiliging**

**Vragenlijst informatieveiligheid en gegevensbescherming voor de verwerker**

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

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

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

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

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

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

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

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

# \*\*\*\*\* EINDE VAN DIT DOCUMENT \*\*\*\*\*

**Annex 4 – Modelformulier melding gegevenslekken**

|  |
| --- |
| Gegevens contactpersoon van het Ziekenhuis (bereikbaar 24/7): |
| Dienst: |
| Telefoonnummer |

|  |
| --- |
| 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. NAW-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 iemand 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 vastgesteld |
| 1. Ten minste …………………………………… (aantal), maar niet meer dan …………………………..(aantal) betrokkenen |
| Omschrijf de groep mensen waarvan persoonsgegevens zijn betrokken bij de inbreuk: |
|  |
| Omstandigheden van de 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 (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 bekend |
|  |
| Zijn de Persoonsgegevens onbegrijpelijk of ontoegankelijk gemaakt voor ongeautoriseerde derden, bijvoorbeeld door encryptie en hashing ? |
| Ja |
| Nee |
| Deels, namelijk |
|  |
| Zo ja, op welke manier zijn de Persoonsgegevens versleuteld: |
|  |
| Heeft de inbreuk betrekking op personen uit andere EU-landen? |
| Ja |
| Nee |
| Zo ja, welke EU-landen: |
|  |
| Welke beveiligingsmaatregelen (technisch en organisatorisch) zijn getroffen om de inbreuk aan te pakken en om verdere inbreuken te voorkomen? |
|  |
| Wie kan benaderd worden voor meer informatie over de inbreuk? |
| Naam contactpersoon van de Leverancier: |
| E-mail : |
| Telefoonnummer: |

**ADDENDUM TO SUPPLIER AGREEMENT CONCERNING DATA PROTECTION**

**Between the undersigned**

[Hospital] with registered office established at …………………………………………………………………., lawfully represented by *[to be completed by department concerned]*

Hereinafter referred to as “**the Hospital**”

AND

…………………………………………………………………………………………………………………………………………………………… [*supplier data to be completed*]

Hereinafter referred to as “**Supplier**”

Hereinafter jointly referred to as the “**Parties**”

**Considering that**

The Supplier provides services for the Hospital, as described in the Basic Agreement, these services entail the processing of personal data and the parties, through this Addendum, wish to establish the arrangements for the processing of personal data in the context of the services

**the following has been agreed:**

**If the Parties wish, by mutual agreement, to make adjustments to the text of this Addendum, such adjustments – in so far as they comply with the Data Protection Legislation and fall within the scope of the contractual freedom of the Parties – shall be recorded, stating the reason, in Annex 1 to this Addendum.**

**Changes to Annex 1 shall be valid only if they have been signed and dated by both parties.**

# Definitions

## For the application of this Addendum, the following definitions shall apply:

### **General Data Protection Regulation**: **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC**, with its amendments and European implementing legislation;

### **Data Protection Legislation**: the General Data Protection Regulation, other European legislation containing provisions concerning data protection and privacy, as well as the applicable national legislation on data protection and privacy in the Member States, with its amendments and implementing decrees, including the approved codes of conduct applicable to the sector.

### **Personal data, Processing, Controller, Processor, Data Subject, Consent**: the definitions as set out in the General Data Protection Regulation;

### **Basic Agreement**: the agreement between the Hospital and the Supplier of ……………………………. [date]  concerning ………………………………………………………………………………………………………… [complete title of agreement, any reference number].

## The Supplier shall provide services to the Hospital on the basis of, and as defined in, the Basic Agreement.

## For the processing activities as specified in **Annex 2** to this Addendum, the following qualification shall apply:

## the Hospital shall determine the purpose and means of processing and shall consequently be the controller;

## the Supplier shall carry out the processing of personal data on behalf of the Hospital as controller, and shall consequently be the processor.

# Scope and relationship to the Basic Agreement

## This Addendum shall form an integral part of the Basic Agreement concluded between the Hospital and the Supplier. The provisions of this Addendum shall apply in full to all processing of personal data performed by the Supplier in the context of the implementation of the processing activities specified in Annex 2.

## The provisions of this Addendum (and Annexes) shall take priority over the (possibly contrary) provisions concerning data protection and processing and confidentiality of data in the Basic Agreement, and shall replace these provisions.

# Processing in accordance with the regulations and the written instructions of the Hospital

## When processing personal data, the Parties shall act in accordance with the Data Protection Legislation.

## The Supplier shall process the personal data exclusively on the basis of the written instructions of the Hospital, unilaterally determined by the Hospital and as set out in **Annex 2** to this Addendum. If the written instructions are not clear, the Supplier shall notify the Hospital of this in writing, whereupon the instructions shall be clarified by common accord.

## Unless otherwise stipulated in this Addendum, the Supplier shall not process the personal data for its own purposes or for those of third parties, or provide the personal data to third parties, or transmit these data to a country located outside the European Union without having received a written instruction to do so from the Hospital. Processing in accordance with the instructions of the Hospital may also mean that the processing must be stopped (immediately).

## If European or national legislation requires the Supplier to undertake specific processing, the Supplier shall inform the Hospital, prior to the processing, of that legal requirement, unless this legislation prohibits such notification for important grounds of general interest.

## The Hospital shall give instructions to the Supplier in accordance with the Data Protection Legislation and shall ensure that all personal data entrusted to the Supplier have been obtained lawfully and can be processed under the Basic Agreement.

# Appropriate technical and organisational measures

## The Parties shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

## When determining the measures, the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of persons, shall be taken into account.

## The measures shall include, inter alia, as appropriate:

## Pseudonymisation and encryption of personal data;

## The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

## The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

## A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

## In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

## The Supplier shall adhere to the standards of approved codes of conduct and certification mechanisms as applicable within the sector. It shall supply evidence thereof in an Annex to this Addendum.

## The Supplier shall describein **Annex 3** the appropriate technical and organisational measures it has implemented. It shall report to the Hospital, on its own initiative, changes made to the measures, as set out in Annex 3, within a period of fourteen days of making the changes.

# Processing by a “Sub-processor” or employee

## The Supplier shall ensure that its representatives, agents, subcontractors and employees comply with the provisions of this Addendum.

## The Supplier shall ensure, in line with this:

## that persons authorised to process personal data have undertaken to maintain confidentiality or are bound by an appropriate statutory obligation of confidentiality;

## that measures have been implemented to ensure that any natural person acting under its authority who has access to the personal data, shall not process these data except on instructions from the Hospital, unless required to process them by European or national legislation.

## .

## The Supplier shall not recruit any other processor (“Sub-processor”) without the prior specific or general written consent of the Hospital.

## In the case of specific written consent, the Supplier shall provide the full details of the processing taken over by the sub-processor in **Annex 1** to this Addendum.

## In the case of general written consent, the Supplier shall make use of a third party as sub-processor only provided that it has informed the Hospital in good time, and in any case in advance, of the identity of the sub-processor and provided that the Hospital has not objected to this.

## If the Supplier has recourse to a sub-processor, the Supplier shall impose on this sub-processor by agreement the same obligations concerning data protection as those applying between Processor and Controller. The Supplier shall provide the Hospital with the agreement with the sub-processor on first request.

## If the sub-processor fails to comply with its data protection obligations, the Supplier shall remain fully liable in relation to the Hospital for complying with the sub-processor’s obligations.

# Provision of assistance with respect to the obligations regarding the data protection policy of the Hospital

## Taking into account the nature of the processing and the information available to it, the Supplier shall undertake to provide assistance to the Hospital with respect to the responsibility of the Hospital to comply with the following data protection obligations:

## Implementation of appropriate technical and organisational measures to ensure a level of security appropriate to the risk;

## Notification of a personal data breach to the supervisory authority;

## Communication of a personal data breach to the data subject;

## Carrying out a data protection impact assessment;

## Consultation of the supervisory authority prior to processing where the data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Hospital to mitigate the risk.

## The time and resources spent by the Supplier in providing the assistance shall be at the Supplier's own expense.

## Pursuant to Article 6.1, the Supplier shall inform the Hospital in detail and immediately of a (suspected) personal data breach as well as of any data leak (at the sub-processor too) as soon as the Supplier has become aware of this. The notification shall take place in such a way that the Hospital can satisfy in time its legal obligations as controller under the Data Protection Legislation. The Supplier shall indemnify the Hospital in accordance with Article 9.2.

## The Supplier shall use the report form in **Annex 4** for the reporting.

The Supplier shall also provide assistance in the investigation and the mitigation and remediation of a personal data breach. In this respect, it shall provide assistance, inter alia, with a view to the documentation of measures such as data protection by design and data protection by default.

## The Supplier shall notify the Hospital immediately of any complaint, accusation or request made (including if it comes from a regulator) with regard to the processing of personal data by the Supplier. The Supplier shall offer all necessary cooperation and support that the Hospital can reasonably expect with regard to such a complaint, accusation or request, including by providing full information on such a complaint, accusation or request, together with a copy of the personal data concerning the data subject in the possession of the Supplier.

# Provision of assistance for requests by the data subjects

## Taking into account the nature of the processing, the Supplier shall provide the Hospital with assistance by appropriate technical and organisational measures in fulfilling the Hospital’s obligation to respond to requests to exercise the rights of the data subject, as specified in the Data Protection Legislation.

## This implies, inter alia:

* + that the Supplier provides all the personal data requested by the Hospital within the (reasonable) period of time requested by the Hospital, in any case including the full details and copies of the complaint, communication or request and any personal data in its possession concerning the data subject;
  + that the Supplier implements technical and organisational measures that permit the Hospital to reply effectively and in a timely manner to relevant complaints, communications or requests.

The time and resources spent by the Supplier in providing the assistance shall be at the Supplier's own expense.

## Pursuant to Article 7.1, the Supplier shall undertake to inform the Hospital without delay if it receives one of the following requests from a data subject (or third party acting on behalf of a data subject):

## a request for access to the data subject’s personal data processed;

## a request for rectification of incorrect personal data;

## a request for erasure of personal data;

## a request for restriction of the processing of personal data;

## a request to obtain a portable copy of the personal data, or for transmission of a copy to a third party;

## an objection to any processing of personal data; or

## any other request, complaint or communication concerning the obligations of the Hospital under the Data Protection Legislation.

The Supplier shall not reply to the requests and applications by the data subject itself, unless there are any written agreements to the contrary between the Hospital and the Supplier.

# Right of control by the Hospital

## The Hospital shall have the right at any time to check compliance by the Supplier with the Addendum.

## The Supplier shall make all information available to the Hospital which is needed to demonstrate compliance with the obligations under the Data Protection Legislation.

## The Supplier shall make audits possible, including inspections, by the Hospital or an auditor authorised by the Hospital, and shall contribute to them. The Supplier shall grant full cooperation with regard to such an audit and, at the request of the Hospital, shall supply evidence of compliance with its obligations under this Addendum.

## The Supplier shall inform the Hospital immediately if, in its opinion, an instruction under Article 8.1 breaches the Data Protection Legislation.

# Liability

## The Parties shall each be responsible and liable for their own actions. The liability regulated in this Article shall relate exclusively to the liability arising from a breach of the Data Protection Legislation and this Addendum.

## The Supplier shall reimburse and indemnify the Hospital for all claims, actions, demands by third parties and for all damage and losses (also including fines imposed by the data protection authority) arising directly or indirectly from processing of personal data if, during the processing, it has not complied with the obligations of the Data Protection Legislation addressed specifically to processors or if it has acted outside or contrary to the lawful instructions of the Hospital.

## The Parties shall ensure sufficient cover of their liability.

# End of the agreement

## If the Supplier fails to comply correctly with the obligations arising from this Addendum or fails to implement appropriate measures within a maximum period of two months, the Hospital – without prejudice to other forms of termination as provided for in the Basic Agreement – may terminate the Basic Agreement immediately after the aforementioned period of two months and/or stop the processing assignment.

## This agreement shall form an integral part of the Basic Agreement and shall therefore follow the fate of the Basic Agreement. However, if the Basic Agreement comes to an end, the provisions of this Addendum shall apply as far as necessary for winding up the obligations in accordance with the Data Protection Legislation.

## Immediately on (no matter which) termination or expiry of the Basic Agreement or after the expiry of the storage period, the Supplier – at the discretion of the Hospital – shall return the personal data to the Hospital and/or irrevocably erase the personal data entirely and remove existing copies. If the Hospital opts for the removal of the personal data, the Supplier shall demonstrate to the Hospital, on written request, that the removal has in fact occurred.

## The Supplier may derogate from paragraph 1 if the storage of the personal data is required under European or national legislation.

# Final provisions

## In the event of nullity or voidability of one or more provisions of this Addendum, the other provisions shall remain in full force.

## This Addendum shall be subject to Belgian law. Disputes shall be brought before the courts/tribunals in the judicial district of Antwerp, Antwerp division, which shall have exclusive territorial jurisdiction.

Thus agreed and drawn up in duplicate at ………………………………………….. on …………………………………….. .

[Name] [Name]

**[The Hospital]** **Supplier**

**Annexes**

Annex 1: Adjustments to the addendum under contractual freedom of the parties

Annex 2: The processing assignment and instructions, as specified by the hospital

Annex 3: Information security

Annex 4: Model form for reporting of data leaks

**Annex 1 – Adjustments to the Addendum under contractual freedom of the parties**

The Addendum contains a standard text which implements the obligations arising from the Data Protection Legislation. Certain aspects fall (within certain limits) under the contractual freedom of the parties.

If the Parties wish to regulate certain aspects differently or more specifically or wish to add certain matters, these are determined explicitly in this Annex.

Contractual freedom can cover, for example:

* the periods within which the Supplier must inform the Hospital or must provide assistance (but in each case within the period within which the Hospital must itself report to the supervisory authority or the department concerned);
* specification of whether specific or general consent is applied for the sub-processor(s);
* …

**Changes in this Annex are valid and enforceable only if this Annex has been signed and dated by both parties.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Article** | **Text which lapses or may lapse** | **Replacement or additional text** | **Reason** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Thus agreed and drawn up in duplicate at ………………………………………….. on …………………………………….. .

[Name] [Name]

**[The Hospital]** **Supplier**

**Annex 2 - The processing assignment and instructions as specified by the Hospital**

***Accompanying note***

*This Annex describes the specific processing by the Supplier, for which the Hospital gives instructions at the time of the conclusion of the Basic Agreement or on signing the Addendum.*

***Changes and/or supplements to this Annex 2 occur in each case via a separate document which is added as an Appendix to this Annex 2 (Appendix 1 to Annex 2; Appendix 2 to Annex 2, etc.), which is dated and which shows the explicit and written instruction and/or agreement of the Hospital.***

**I. The purpose of the processing of personal data**

The processing of Personal Data by the Supplier takes place under the implementation of the Basic Agreement concerning…………………………………………………………………………. *[to be completed by supplier]*.

Description of the services under the Basic Agreement and nature and purpose of the processing of personal data in the context of the services:

…………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………….

**II. The categories of personal data which the Hospital instructs the Supplier to process (indicate what is applicable and if necessary supplement):**

* contact details
* financial data
* invoice data
* wage data
* medical data
* marketing data
* data on the use by the Hospital of the services and related products of the Supplier
* other (to be specified):

…………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………….

**III. The categories of data subjects whose personal data are processed (indicate what is applicable and if necessary supplement):**

* Hospital patients
* trusted persons, representatives and contact persons of the Hospital patients
* carers of the Hospital patients
* Hospital staff members
* other (to be specified):

………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………….

**IV. The processing of the personal data (indicate what is applicable and adapt/supplement where necessary):**

The Hospital hereby gives the following instructions for the processing of personal data (without prejudice to the instructions arising directly from the provisions of the Basic Agreement or this Addendum or which are reasonably required for the Supplier to fulfil its obligations correctly):

* Consultation of personal data

This refers to services provided by the Supplier whereby personal data of the Hospital can be viewed by staff or Subcontractors of the Supplier, including, but not limited to, servicedesk Services, (remote) monitoring Services, system management Services, technical application management, vulnerability scanning Services, reporting Services in governance and software asset management Services.

* Storage of personal data

This refers to services provided by the Supplier whereby personal data of the Hospital are stored in a storage system delivered by the Supplier, such as, but not limited to, cloud storage Services, cloud back-up Services, file Services, directory Services, managed file transfer, mail & calendaring and logfile processing.

* Transmission of personal data

This refers to services provided by the Supplier whereby personal data of the Hospital are transmitted by, to or between applications on a platform managed by the Supplier, including, but not limited to, LAN Services, Wide Area Network Services, data centre interconnectivity Services, Loadbalancing, SAN switch interconnects and Services provided using the Voice over Internet Protocol (VoIP).

* Adaptation or alteration of personal data

This refers to services provided by the Supplier whereby personal data of the Hospital can be adapted either manually or automatically, such as in an automated job flow supported by a job scheduling system.

* Software tests

This refers to services provided by the Supplier in which databases of the Hospital containing personal data (personal data which have not been anonymised) are used outside the production environment (in test, acceptance, etc.) as part of the testing process of the Hospital software application.

* XXX
* XXX
* XXX
* XXX
* [To be completed]

**IV. The storage periods of the (various categories of) personal data:**

The Supplier stores the processed personal data in an appropriately secure manner for the period necessary to perform the written instructions of the Hospital, and with regard to the categories of personal data below, for the period specified below **[complete if storage period can be expressed in months]**:

* for **[complete category of data]** for **[ XX months after/from…. e.g. the last use]**
* for **[complete category of data]** for **[ XX months after/from…. e.g. the last use]**

**V. The Data Protection Officer or other responsible contact persons for data protection and processing (complete):**

**For the Hospital**

Name:

Contact details:

**For the Supplier**

Name:

Contact details:

**Annex 3 – Information security**

**Questionnaire on information security and data protection for the processor**

|  |  |
| --- | --- |
| Name of the organisation (third party) | Name: .............................................................................  Address: .............................................................................  .............................................................................  Business number (Crossroads Bank):  ............................................................................. |
| First name, Surname & e-mail address of the chief information security officer (CISO) (mandatory) | ...........................................................................................  ........................................................................................... |
| First name, Surname & e-mail address of the information security contact person (assistant CISO) (optional) | ...........................................................................................  ........................................................................................... |
| First name, Surname & e-mail address of the data protection officer (DPO) (mandatory) | ...........................................................................................  ........................................................................................... |
| First name, Surname & e-mail address of the local data protection contact person (assistant DPO or representative) (optional) | ...........................................................................................  ........................................................................................... |
| First name, Surname & e-mail address of the person responsible for day-to-day management (CEO, mandatory) | ...........................................................................................  ........................................................................................... |

|  |  |  |  |
| --- | --- | --- | --- |
| Question | *Place cross (X) in the box corresponding to your answer* | | Explain in the case of a ‘no’ response |
| 1 | Do you have a formal, up-to-date information security policy approved by the person responsible for day-to-day management? | YES NO |  |
| 2 | Do you have a risk assessment for each process/project for information security/data protection which you use for the provision of services? | YES NO |  |
| 3 | Within your organisation:   * is there a department responsible for information security reporting directly to the person responsible for day-to-day management of the organisation? | YES NO      YES NO |  |
| 4 | Do you have an information security plan approved by the person responsible for day-to-day management? | YES NO |  |
| 5 | How many hours are worked by the CISO and his/her team?   * CISO * Team   How many hours of training on information security have the DPO and his/her team followed?   * DPO * Team | 1. hours / month 2. hours / month 3. hours /year 4. hours /year |  |
| 6 | Do you have procedures for the development of new systems or major changes to existing systems so that the project leader can take account of the security requirements described in the minimum security standards? | YES NO N/A |  |
| 7 | Do you take appropriate measures so that the professional, confidential and sensitive data stored on mobile media are accessible only to authorised persons? | YES NO |  |
| 8 | Do you take appropriate measures, depending on the access medium, for the information security of the access from outside your organisation to the professional, confidential and sensitive data? | YES NO |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Question | *Place cross (X) in the box corresponding to your answer* | | Explain in the case of a ‘no’ response |
| 9 | Do you have teleworking facilities arranged in such a way that at the teleworking location (at home, in a satellite office or in another location) no information is stored on external appliances without encryption and that possible threats from the teleworking location do not reach the IT infrastructure? | YES NO |  |
| 10 | Do you call the attention of each staff member each year to information security and data protection and do you carry out an annual evaluation of compliance with this policy in practice? | YES NO |  |
| 11 | Have you secured access by means of a clear access procedure and have you implemented a (logical or physical) access system to prevent any unauthorised access? | YES NO |  |
| 12 | Do you have a classification system for personal data for which you are providing the services and do you apply this classification system? | YES NO |  |
| 13 | Have you processed the rules, specified in an ‘E-mail, online communication and internet use’ policy line, in an information security policy? | YES NO |  |
| 14 | Have you appointed at least one access manager when you make use of remote access to the healthcare institution? | YES NO |  |
| 15 | Have you encouraged your staff to read and apply extra security measures which the care provision imposes (if applicable)? | YES NO |  |
| 16 | If you wish to apply ‘cryptography’:   * do you have a formal policy for the use of cryptographic controls? * do you have a formal policy for the use, protection and life of cryptographic keys for the entire lifecycle? | YES NO      YES NO |  |
| 17 | Do you take the necessary measures to limit access to the buildings and premises to authorised persons and do you monitor this access both during and outside working hours? | YES NO |  |
| 18 | Do you take the necessary measures to prevent loss, damage, theft or compromise of equipment and interruption of the activities? | YES NO |  |
| 19 | In the case of reuse of the information carrier, do you use it again at a data classification level which is at least comparable? | YES NO |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Question | *Place cross (X) in the box corresponding to your answer* | | Explain in the case of a ‘no’ response |
| 20 | Do you establish appropriate measures for the erasure of data contractually with the principal? | YES NO |  |
| 21 | Do you apply the rules relating to logging of access as stipulated by the principal? | YES NO |  |
| 22 | Have rules been laid down for the acquisition, development and maintenance of systems between the various parties concerned? | YES NO |  |
| 23 | Do all staff members work with ICT resources for the purposes of the assignment on the basis of minimum authorisation for the performance of their task? | YES NO |  |
| 24 | Have the access security requirements (identification, authentication, authorisation) been defined, documented, validated and communicated? Are these accesses logged? | YES NO      YES NO |  |
| 25 | Are the security and data protection risks established contractually between you and any subcontractors? | YES NO |  |
| 26 | Do you use a checklist so that the project leader can obtain the assurance that all the information security and data protection policy lines have been evaluated correctly and if necessary implemented during the development phase of the project? | YES NO |  |
| 27 | Each time a project is put into production, do you carry out a check that the security and data protection requirements laid down at the beginning of the project were also in fact implemented? | YES NO |  |
| 28 | Under the supervision of the project leader, are there separated facilities for development, testing and/or acceptance and production – including the related separation of the responsibilities under the project? | YES NO |  |
| 29 | Is each access to personal and confidential data logged in accordance with a logging policy and the applicable laws and regulations? | YES NO |  |
| 30 | Is it included in project specifications how access to and use of systems and applications will be logged to contribute to the detection of divergences with regard to information security and data protection? | YES NO |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Question | | | *Place cross (X) in the box corresponding to your answer* | | | Explain in the case of a ‘no’ response | | |
| 31 | | | Does the log management at least comply with the following objectives?   * The information to be able to determine by whom, when and how access was obtained to which information * The identification of the nature of the information consulted * The clear identification of the person | YES NO | | |  | |
| 32 | | | Have the necessary tools been made available to allow the log data to be operated by the authorised persons? | YES NO | | |  | |
| 33 | | | Do the transactional/functional log data correspond to the storage period corresponding to the data themselves (e.g. 30 years for medical data)? | YES NO | | |  | |
| 34 | | | Are the project deliverables (processed data, documentation (source code, programs, technical documents, etc.) integrated in the back-up management system? | YES NO | | |  | |
| 35 | | | In the course of the project development, have the requirements with regard to continuity of service provision been formalised, in accordance with your expectations? | YES NO | | |  | |
| 36 | | | Have your continuity plan and the related procedures been updated in line with the development of the project, including continuity tests? | YES NO | | |  | |
| 37 | | | Is a risk analysis carried out at the beginning of the project to define the emergency procedures? | YES NO | | |  | |
| 38 | | | In the course of the project development, are the procedures concerning incident management formalised and validated? | YES NO | | |  | |
| 39 | | | Is the CISO informed of security incidents and the DPO for incidents concerning data protection? | YES NO | | |  | |
| 40 | | | During the lifecycle of the project, is the documentation (technical, procedures, manuals, etc.) kept up to date? | YES NO | | |  | |
| 41 | | | Is all equipment, including purchased or developed systems added to the inventory of the operational resources? | YES NO | | |  | |
| 42 | | | Is appropriate cooperation given to audits carried out in the form of the personnel being made available, documentation, log management and other information which is reasonably available? | YES NO | | |  | |
| 43 | | | Are requirements concerning information security and data protection documented to mitigate risks concerning access to information tools? | YES NO | | |  | |
| 45 | | | Are all relevant requirements concerning information security and privacy drawn up and agreed between you and third parties/suppliers (who | YES NO | | |  | |
| Question | *Place cross (X) in the box corresponding to your answer* | | | | | | Explain in the case of a ‘no’ response | |
|  | read, process, store, communicate information of the organisation or supply ICT infrastructure components and ICT services)? | | |  | | |  | |
| 46 | Are the services provided to you by third parties/suppliers monitored, evaluated and audited? | | | YES NO | | |  | |
| 47 | Are the changes in the provision of services to you by the third party/supplier managed, including keeping records of existing policy lines, procedures/measures for information security and data protection? | | | YES NO | | |  | |
| 48 | Do you have a ‘Cloud computing’ policy line when you call on cloud services? | | | YES NO | | |  | |
| 49 | When you wish to process professional, confidential or sensitive data in a cloud, do you satisfy the minimum contractual guarantees? | | | YES NO | | |  | |
| 50 | Do you have procedures for establishment and management of incidents relating to information security or data protection with the related responsibilities and have you made these procedures known in-house? | | | YES NO | | |  | |
| 51 | Do you have an agreement with all staff members that each staff member (permanent or temporary, in-house or external) is required to report unauthorised access, use, alteration, disclosure, loss or destruction of information and information systems? | | | YES NO | | |  | |
| 52 | Are the incidents and weaknesses of information security or data protection relating to information and information systems made known to the principal so that you and the principal can take appropriate corrective measures in good time? | | | YES NO | | |  | |
| 53 | Does the supplier have a procedure to communicate/report incidents concerning information security/data protection in-house as quickly as possible? | | | YES NO | | |  | |
| 54 | In the case of information security or data protection incidents, is the evidence collected correctly in accordance with statutory and regulatory requirements? | | | YES NO | | |  | |
| 55 | Is each information security or data protection incident formally validated so that procedures and control measures can be improved and are the lessons drawn from an incident communicated to your management for validation and approval of further actions? | | | YES NO | | |  | |

|  |  |  |  |
| --- | --- | --- | --- |
| Question | *Place cross (X) in the box corresponding to your answer* | | Explain in the case of a ‘no’ response |
| 56 | Do you have a continuity plan for all critical processes and essential information systems? | YES NO |  |
| 57 | Are information security and data protection an integral part of your continuity management? | YES NO |  |
| 58 | Do you have your own continuity plan?  Is this plan tested and adapted regularly with the necessary communication to your management for validation and approval? | YES NO      YES NO |  |
| 59 | Do you carry out a conformity audit periodically with regard to the situation concerning information security and data protection? | YES NO |  |
| 60 | Do you have a formal disciplinary process for employees who have breached information security and data protection? | YES NO |  |
| 61 | Do you regularly collate all information to map the risks in connection with conformity with the GDPR and do you take the necessary actions as a result of a high ‘residual’ risk of non-conformity? | YES NO |  |
| 62 | Do you have an up-to-date central register of the controller or of the processor and do you have formal accountability for non-implementation of control measures focusing on compliance with the European Regulation for the specific processing? | YES NO |  |

|  |  |
| --- | --- |
| Date and signature of the CISO or data management officer (DPO) of the organisation (third party) (optional) | ...........................................................................................  Date Signature |
| Date and signature of the person responsible for the day-to-day management of the organisation (third party) **(mandatory)** | ...........................................................................................  Date Signature |

# \*\*\*\*\* END OF THIS DOCUMENT \*\*\*\*\*

**Annex 4 – Model form for reporting of data leaks**

|  |
| --- |
| Details of contact person of the Hospital (contactable 24/7): |
| Department: |
| Telephone number |

|  |
| --- |
| Date: |
|  |
| Company name: |
| Address: |
| Postcode: |
| VAT number |
|  |
| Who found the breach? |
| Name: |
| Job title: |
|  |
| When was the breach found? |
| Date: |
| Time: |
|  |
| Describe the security incident during which the breach of security of personal data occurred: |
| When did the breach take place? |
| 1. On (date + time) |
| 1. Between (date + time) and (date + time) |
| 1. Not yet established |
| 1. An anonymous report has been made by a third party |
|  |
| Establish context of the data involved in the breach: |
| Classification of the data: |
| 1. None, the data cannot be attributed to an individual |
| 1. Name and address data |
| 1. Telephone numbers |
| 1. E-mail addresses, Facebook IDs, Twitter IDs, etc. |
| 1. User names, passwords or other login data, customer numbers |
| 1. Financial data: account numbers, credit card numbers |
| 1. National registration number |
| 1. Copies of identity documents |
| 1. Gender, data of birth, and/or age |
| 1. Data concerning someone’s religion or philosophy of life, race, political persuasion or membership of a trade union |
| 1. Data concerning someone’s health or sexual orientation |
| 1. Personal data under criminal law or personal data about unlawful or annoying behaviour in connection with a prohibition imposed as a result of that behaviour |
| 1. Data about someone’s financial or economic situation, data on debts, salary and payment data |
| 1. Derived financial data (income category, home ownership, car ownership) |
| 1. Lifestyle characteristics (including family composition, housing situation, interests, demographic characteristics (age, gender, nationality, profession, education) |
| 1. Data obtained from (public) social profiles (Facebook, LinkedIn and Twitter accounts, etc.) |
| 1. Other, namely: |
|  |
| Classification of the context involved in the breach: |
| The breach involves the personal data of how many persons? |
| 1. None, the data cannot be attributed to an individual |
| 1. Not yet established |
| 1. At least …………………………………… (number), but no more than …………………………..(number) involved |
| Describe the group of people whose personal data were involved in the breach: |
|  |
| Circumstances of the data leak: |
| 1. Read only (an unauthorised third party was able to inspect (confidential) data. Processor still has the data in its possession.) – Confidentiality is at risk |
| 1. Copy (an unauthorised third party was able to copy data. The data are still in the possession of Processor.) – Confidentiality is at risk |
| 1. Alteration (an unauthorised third party was able to alter data in systems of the Processor – Integrity is at risk |
| 1. Removal or destruction (an unauthorised third party removed data from the systems of the Processor or destroyed data.) – Availability is at risk |
| 1. Theft – Availability is at risk |
| 1. Not yet known |
|  |
| Were the Personal Data made incomprehensible or inaccessible for unauthorised third parties, for example by encryption and hashing? |
| Yes |
| No |
| Partly, i.e. |
|  |
| If so, how were the Personal Data encrypted? |
|  |
| Did the breach involve persons from other EU Member States? |
| Yes |
| No |
| If so, which EU Member States: |
|  |
| Which security measures (technical and organisational) have been implemented to tackle the breach and to prevent further breaches? |
|  |
| Who can be contacted for more information on the breach? |
| Name of contact person of the Supplier: |
| E-mail: |
| Telephone number: |