HAN_UNIVERSITY OF APPLIED SCIENCES

Model Verwerkersovereenkomst[1]

DE ONDERGETEKENDEN:

Stichting Hogeschool van Arnhem en Nijmegen, gevestigd aan de Ruitenberglaan 31, 6826 CC te Arnhem, ingeschreven in Handelsregister, Kamer van Koophandel nummer 09091785, en rechtsgeldig vertegenwoordigd door <…….>, hierna te noemen "**Verwerkingsverantwoordelijke**";

en

<NAAM LEVERANCIER/VERWERKER>, gevestigd aan <ADRES……..> te <PLAATS…….>, en rechtsgeldig vertegenwoordigd door <VERTEGENWOORDIGER……> hierna: "**Verwerker**,;

hierna gezamenlijk: "**Partijen**" en individueel ook: "**Partij**";

NEMEN HET VOLGENDE IN AANMERKING:

- Partijen hebben op <DATUM ……..> een overeenkomst (schriftelijk of op elektronische wijze waaronder via een elektronisch (bestel)proces) gesloten met betrekking tot <ONDERWERP VAN DE OVEREENKOMST……..> (hierna: "**Overeenkomst**");

- bij de uitvoering van de Overeenkomst verwerkt Verwerker ten behoeve van Verwerkingsverantwoordelijke persoonsgegevens;

- Partijen wensen in overeenstemming met de Algemene Verordening Gegevensbescherming (AVG) hun rechten en plichten ten aanzien van het verwerken van deze persoonsgegevens van betrokkenen schriftelijk vast te leggen in deze verwerkersovereenkomst (hierna: "**Verwerkersovereenkomst**");

EN ZIJN ALS VOLGT OVEREENGEKOMEN:

ARTIKEL 1 DEFINITIES EN VARIA

1.1 In deze Verwerkersovereenkomst betekenen de met hoofdletter geschreven termen hetzelfde als in artikel 4 AVG, tenzij anders gedefinieerd.

1.2 De bepalingen van deze Verwerkersovereenkomst zijn van toepassing op alle Verwerkingen van de Persoonsgegevens die Verwerker uitvoert ten behoeve van Verwerkingsverantwoordelijke in het kader van de diensten die hij levert aan

[1] Dit model is gebaseerd op de modelovereenkomst van SURF (verwerkersovereenkomst 4.0 voor het onderwijs, november 2024). Te vinden op https://pec.surf.nl/asset/surf-model-verwerkersovereenkomst-v4-0-nl/

Verwerkingsverantwoordelijke op grond van de Overeenkomst. In Bijlage A zijn deze Persoonsgegevens en Verwerkingen opgenomen en nader omschreven.

1.3 De in dit document genoemde bijlagen en de latere aanpassingen en aanvullingen daarvan zijn een onderdeel van deze Verwerkersovereenkomst.

ARTIKEL 2 DOEL VAN DE VERWERKERSOVEREENKOMST

2.1 Verwerker verwerkt de Persoonsgegevens alleen:

(i) in opdracht van Verwerkingsverantwoordelijke,
(ii) volgens zijn redelijke schriftelijke instructies, en
(iii) voor zover de Verwerking noodzakelijk is voor de uitvoering van de Overeenkomst en deze Verwerkersovereenkomst.

2.2 Verwerker verricht alle Verwerkingen van de Persoonsgegevens in overeenstemming met de AVG en de andere toepasselijke wet- en regelgeving op het gebied van gegevensbescherming, bijvoorbeeld de Uitvoeringswet AVG en de Telecommunicatiewet (hierna: "**Toepasselijke Wetgeving**").

2.3 Verwerker informeert Verwerkingsverantwoordelijke onmiddellijk als:

(i) een instructie van Verwerkingsverantwoordelijke in strijd is met de AVG en/of Toepasselijke Wetgeving;
(ii) Verwerker niet langer aan deze Verwerkersovereenkomst kan voldoen;
(iii) Verwerker op grond van een wettelijke verplichting de Persoonsgegevens moet verwerken, tenzij deze informatieverstrekking op basis van de wet verboden is.

ARTIKEL 3 VERLENEN VAN MEDEWERKING

3.1 Op verzoek van Verwerkingsverantwoordelijke werkt Verwerker direct mee aan het nakomen van de verplichtingen die Verwerkingsverantwoordelijke ter zake van de Persoonsgegevens heeft op grond van de AVG en Toepasselijke Wetgeving. Die medewerking, in deze Verwerkersovereenkomst op een aantal onderwerpen nader uitgewerkt, heeft betrekking op onder meer:

(i) voldoen aan verzoeken van Betrokkenen;
(ii) uitvoeren van Data Protection Impact Assessments (DPIA's) en voorafgaande raadpleging bij Toezichthoudende autoriteiten;
(iii) uitvoeren van Data Transfer Impact Assessments (DTIA's);
(iv) voldoen aan verzoeken van (inter)nationale (overheids-)instanties.

3.2 Als Verwerker een verzoek krijgt van een (inter)nationale (overheids-) instantie over de Persoonsgegevens, dan:

(i) neemt Verwerker direct contact op met Verwerkingsverantwoordelijke, en
(ii) volgt Verwerker de instructies van Verwerkingsverantwoordelijke op.

ARTIKEL 4 SUBVERWERKERS

4.1 Verwerkingsverantwoordelijke geeft Verwerker algemene toestemming voor het inschakelen van een andere verwerker in de zin van artikel 28 lid 4 AVG (hierna: "**Subverwerkers**"). De door Verwerker ingeschakelde Subverwerkers zijn opgenomen in

Bijlage A. Bij beoogde wijzigingen van de Subverwerkers zal Verwerker het proces in artikel 12.3 volgen.

4.2 Verwerker blijft volledig aansprakelijk jegens Verwerkingsverantwoordelijke voor het nakomen van de verplichtingen door Subverwerkers.

4.3 Verwerker legt Subverwerkers contractueel de verplichtingen uit deze Verwerkersovereenkomst op. Op verzoek verstrekt Verwerker Verwerkingsverantwoordelijke een kopie van deze contractueel overeengekomen verplichtingen. Het is Verwerker toegestaan concurrentiegevoelige informatie weg te laten in de kopie die hij verstrekt aan Verwerkingsverantwoordelijke.

ARTIKEL 5 GEHEIMHOUDING

5.1 Verwerker is verplicht tot geheimhouding van de Persoonsgegevens. Personen die voor Verwerker werken hebben een geheimhoudingsverklaring getekend, of zijn op een andere manier gebonden aan geheimhouding. Verwerkingsverantwoordelijke kan hiervan bewijs vragen.

5.2 De geheimhouding kan worden doorbroken als dit noodzakelijk is voor de uitvoering van de Overeenkomst of deze Verwerkersovereenkomst, door Toepasselijke Wetgeving, een uitspraak van een Nederlandse rechter of een rechter in een andere EU-lidstaat. In geval van een rechterlijke uitspraak uit een derde land, treedt Verwerker eerst in overleg met Verwerkingsverantwoordelijke alvorens de Persoonsgegevens te verstrekken.

ARTIKEL 6 BEVEILIGING

6.1 Verwerker neemt passende technische en organisatorische maatregelen in de zin van artikel 32 AVG om de Persoonsgegevens te beveiligen. De maatregelen die Verwerker heeft geïmplementeerd, zijn opgenomen in Bijlage B.

6.1.1 Verwerker evalueert en actualiseert de beveiligingsmaatregelen periodiek om te waarborgen dat deze blijven voldoen aan de stand van de techniek en een passend beschermingsniveau bieden. Verwerker waarborgt dat wijzigingen in de beveiligingsmaatregelen niet leiden tot een lager beveiligingsniveau dan overeengekomen bij aanvang van de Verwerkersovereenkomst of later schriftelijk afgesproken. Verwerker is gerechtigd om Bijlage B eenzijdig aan te passen aan de meest recente beveiligingsstandaarden. Verwerker informeert Verwerkingsverantwoordelijke schriftelijk over wijzigingen in Bijlage B.

6.2 Verwerker documenteert zijn beveiligingsbeleid schriftelijk en toont op verzoek van Verwerkingsverantwoordelijke bewijs van het bestaan van de getroffen maatregelen. Verwerkingsverantwoordelijke behandelt deze informatie vertrouwelijk, behalve als openbaarmaking vereist is door een rechterlijk bevel of als een Toezichthoudende autoriteit dit verzoekt.

ARTIKEL 7 INBREUK IN VERBAND MET PERSOONSGEGEVENS

7.1 Als bij Verwerker een Inbreuk in verband met persoonsgegevens (hierna: "**Inbreuk**") plaatsvindt, of als daarvan een redelijk vermoeden bestaat, informeert Verwerker Verwerkingsverantwoordelijke onmiddellijk en binnen 24 uur na ontdekking van de Inbreuk. Verwerker geeft bij het informeren minimaal de informatie uit Bijlage C aan de contactpersoon genoemd in die bijlage. Als het voor Verwerker niet mogelijk is al deze

informatie meteen te geven, zal Verwerker deze informatie stapsgewijs aan Verwerkingsverantwoordelijke verstrekken.

7.2 Verwerker meldt Inbreuken niet aan de Toezichthoudende autoriteit en/of de getroffen Betrokkenen, tenzij Verwerkingsverantwoordelijke daar uitdrukkelijk schriftelijk om vraagt.

7.3 Verwerker neemt zo snel mogelijk maatregelen om de oorzaken van de Inbreuk weg te nemen en de mogelijke nadelige gevolgen van de Inbreuk zoveel mogelijk te verminderen of ongedaan te maken.

7.4 Partijen houden de contactgegevens in Bijlage C actueel en sturen steeds de actuele versie naar de andere Partij.

7.5 Verwerker heeft beleid en procedures om: (i) Inbreuken zo vroeg mogelijk op te sporen, (ii) Verwerkingsverantwoordelijke volgens artikel 7.1 te informeren, (iii) snel te reageren op een Inbreuk, (iv) ongeoorloofde toegang, wijziging of verspreiding van de Persoonsgegevens te voorkomen en te beperken en (v) herhaling van de Inbreuk te voorkomen.

7.6 Verwerker geeft informatie over dit beleid en deze procedures als Verwerkingsverantwoordelijke daarom vraagt.

7.7 Verwerker houdt een register bij van alle Inbreuken gerelateerd aan de Verwerkingen van de Persoonsgegevens, met details over deze Inbreuk, gevolgen en genomen (corrigerende) maatregelen. Verwerker geeft Verwerkingsverantwoordelijke een kopie van dit register als deze daarom vraagt.

ARTIKEL 8 AUDIT

8.1 Verwerker stelt aan Verwerkingsverantwoordelijke alle informatie ter beschikking die nodig is om de naleving van de verplichtingen uit deze Verwerkersovereenkomst aan te tonen. Verwerker stelt jaarlijks een auditrapport op waarin hij aantoont dat hij voldoet aan de verplichtingen uit deze Verwerkersovereenkomst en verstrekt deze op verzoek. Dit rapport wordt opgesteld door een onafhankelijke, deskundige derde partij en is voorzien van een verklaring dat de bevindingen een getrouw beeld geven van de werkelijkheid. Indien concrete omstandigheden naar het oordeel van Verwerkingsverantwoordelijke daartoe aanleiding geven of indien Verwerkingsverantwoordelijke vermoedt dat Verwerker zijn verplichtingen niet nakomt, kan Verwerkingsverantwoordelijke alsnog een eigen audit (laten) uitvoeren. Verwerker zal daar zijn medewerking aan verlenen, onder meer door het verlenen van toegang tot systemen en documenten. De kosten van een eigen audit zijn voor rekening van Verwerkingsverantwoordelijke, tenzij uit de audit blijkt dat Verwerker tekort is geschoten in de nakoming van zijn verplichtingen uit deze Verwerkersovereenkomst.

8.2 Verwerkingsverantwoordelijke meldt de audit minstens veertien (14) dagen van tevoren. De audit zal de normale bedrijfsactiviteiten van Verwerker niet onredelijk verstoren.

8.3 Verwerkingsverantwoordelijke behandelt de uit de audit verkregen informatie vertrouwelijk en deelt deze alleen met die samenwerkingspartners voor wie kennisname van de informatie redelijkerwijs noodzakelijk is. Verwerkingsverantwoordelijke noch de hiervoor bedoelde samenwerkingspartners zullen de auditresultaten openbaar maken of met derden delen, tenzij dit wettelijk vereist is.

8.4 Als uit de audit blijkt dat Verwerker niet aan zijn verplichtingen uit deze Verwerkersovereenkomst voldoet, neemt Verwerker direct en op eigen kosten alle redelijke maatregelen om te zorgen dat Verwerker alsnog aan deze verplichtingen voldoet.

ARTIKEL 9 DOORGIFTE VAN PERSOONSGEGEVENS

9.1 Verwerker mag de Persoonsgegevens alleen doorgeven aan een land buiten de Europese Economische Ruimte of een internationale organisatie als: (i) wordt voldaan aan de artikelen 44 tot en met 49 AVG, en (ii) Verwerkingsverantwoordelijke tijdig schriftelijk wordt geïnformeerd voordat de doorgifte begint. De doorgiften die plaatsvinden, zijn opgenomen in Bijlage A. Bij beoogde wijzigingen van de doorgiften in Bijlage A zal Verwerker het proces in artikel 12.3 volgen.

9.2 Indien een doorgifte plaatsvindt op basis van een adequaatheidsbesluit van de Europese Commissie, de standaardbepalingen voor doorgifte of bindende bedrijfsvoorschriften, verwijzen Partijen in Bijlage A naar de specifieke relevante documenten of hechten deze als bijlage aan deze Verwerkersovereenkomst.

9.3 Als sprake is van een wijziging of aanvulling van de vereisten inzake doorgiften, bijvoorbeeld door rechterlijke uitspraken, nieuwe of gewijzigde adequaatheidsbesluiten/model clausules van de Europese Commissie of aanbevelingen van Toezichthoudende autoriteiten, neemt Verwerker maatregelen om te voldoen aan deze gewijzigde of aangevulde vereisten.

ARTIKEL 10 VERZOEK TOEGANG PERSOONSGEGEVENS[2]

10.1 Indien de Verwerker een juridisch bindend verzoek ontvangt van een (buitenlandse) autoriteit om toegang te verkrijgen tot persoonsgegevens, stelt de Verwerker de Verwerkingsverantwoordelijke hiervan onverwijld en voorafgaand aan de verstrekking op de hoogte, tenzij dit wettelijk verboden is.

10.2 De Verwerker verbindt zich ertoe alle redelijke juridische middelen aan te wenden om dergelijke verzoeken aan te vechten die in strijd zijn met het toepasselijke recht van de Europese Unie of de lidstaat waarin de Verwerkingsverantwoordelijke is gevestigd.

10.3 Indien de Verwerker op grond van buitenlands recht (waaronder de U.S. CLOUD Act) gehouden is gegevens te verstrekken, en hij de Verwerkingsverantwoordelijke niet kan informeren, zal hij zich beperken tot de minimaal vereiste gegevensverstrekking en aantonen dat hij passende maatregelen heeft genomen om de inbreuk op de rechten van betrokkenen zo veel mogelijk te beperken.

10.4 De Verwerker houdt een register bij van alle verzoeken van (buitenlandse) autoriteiten tot toegang tot persoonsgegevens, inclusief de aard van het verzoek, de juridische grondslag, de omvang van de verstrekte gegevens en de genomen maatregelen. Dit register wordt desgevraagd verstrekt aan de Verwerkingsverantwoordelijke.

[2] Dit artikel is extra toegevoegd mede in verband met de U.S. CLOUD Act.

10.5 De Verwerker is aansprakelijk jegens de Verwerkingsverantwoordelijke voor schade die voortvloeit uit het zonder geldige juridische grondslag verstrekken van persoonsgegevens aan (buitenlandse) autoriteiten.

ARTIKEL 11 VRIJWARING EN AANSPRAKELIJKHEID

11.1 Verwerker vrijwaart Verwerkingsverantwoordelijke tegen alle vorderingen, boetes, verliezen, schaden en onkosten die voortvloeien uit, of verband houden met, schending door Verwerker van deze Verwerkersovereenkomst. Deze vrijwaring heeft voorrang op de afspraken rond vrijwaring, aansprakelijkheid en schadevergoeding in de Overeenkomst.

11.2 Verwerker heeft voor de aansprakelijkheid zoals bedoeld in artikel 11.1 een geldige aansprakelijkheidsverzekering met een verzekerd bedrag van EUR 1.000.000,- (een miljoen euro) per gebeurtenis en EUR 2.000.000,- (twee miljoen euro) per jaar. Verwerker verstrekt op verzoek van Verwerkingsverantwoordelijke een exemplaar van (het certificaat van) de polis en polisvoorwaarden.

ARTIKEL 12 WIJZIGING

12.1 Partijen kunnen deze Verwerkersovereenkomst, met uitzondering van de in deze Verwerkersovereenkomst beschreven wijzen van aanpassing van de bijlagen, alleen wijzigen of aanvullen met een schriftelijke overeenkomst die door beide Partijen is ondertekend.

12.2 Wijzigingen of aanvullingen van deze Verwerkersovereenkomst mogen niet in strijd zijn met de Toepasselijke Wetgeving.

12.3 Ingeval van voorgenomen wijzigingen van Subverwerkers en van doorgiften buiten de EER, zal Verwerker het volgende in acht nemen:

a. Verwerker informeert Verwerkingsverantwoordelijke schriftelijk en zo vroeg mogelijk over voorgenomen wijzigingen.
b. Verwerker actualiseert Bijlage A met de voorgenomen wijzigingen.
c. Verwerkingsverantwoordelijke heeft na ontvangst van het wijzigingsverzoek en de actualiseerde Bijlage A een (1) maand om schriftelijk gemotiveerd bezwaar te maken.
d. Bij bezwaar treden Partijen in overleg. De voorgenomen wijzigingen zijn niet van kracht voordat Partijen overeenstemming hebben bereikt.
e. Wordt binnen twee (2) maanden na bezwaar geen oplossing gevonden, kan Verwerkingsverantwoordelijke de Overeenkomst opzeggen met een (1) maand opzegtermijn, zonder daarbij tot vergoeding van kosten of schadevergoeding gehouden te zijn.
f. Maakt Verwerkingsverantwoordelijke niet tijdig bezwaar, dan wordt de voorgenomen wijziging geacht te zijn geaccepteerd na afloop van de bezwaartermijn genoemd onder c van deze bepaling.

12.4 Als zich een wijziging voordoet in de zeggenschap over Verwerker, bijvoorbeeld door een fusie, overname of wijziging van de eigendomstructuur, informeert Verwerker Verwerkingsverantwoordelijke hierover zo spoedig mogelijk. Verwerkingsverantwoordelijke heeft in dat geval het recht om de Overeenkomst schriftelijk op te zeggen met inachtneming

van een opzegtermijn van minimaal drie (3) maanden.

ARTIKEL 13 INGANGSDATUM, DUUR EN BEËINDIGING

13.1 Deze Verwerkersovereenkomst gaat in als Partijen deze Verwerkersovereenkomst hebben ondertekend. Als de Verwerking van de Persoonsgegevens al is begonnen voordat deze Verwerkersovereenkomst is ondertekend, geldt deze Verwerkersovereenkomst met terugwerkende kracht met ingang van de datum waarop de Verwerking is gestart.

13.2 Deze Verwerkersovereenkomst is niet los van de Overeenkomst te beëindigen.

13.3 Binnen een (1) maand nadat de Overeenkomst op welke grond dan ook eindigt, vernietigt of retourneert Verwerker alle Persoonsgegeven (en eventueel kopieën bij Subverwerkers). Kiest Verwerkingsverantwoordelijke voor teruggave, dan draagt Verwerker deze in een gangbaar format over aan Verwerkingsverantwoordelijke of aan een andere partij die Verwerkingsverantwoordelijke aanwijst. Indien in Bijlage A een afwijkende bewaartermijn is opgenomen in relatie tot specifieke Verwerkingen van de Persoonsgegevens, prevaleert die termijn boven de termijn uit dit artikel.

13.4 De verplichtingen voor Verwerker uit deze Verwerkersovereenkomst blijven gelden tot het moment dat Verwerker geen Verwerkingen van de Persoonsgegevens meer verricht.

13.5 Verwerker bevestigt schriftelijk aan Verwerkingsverantwoordelijke dat hij aan alle verplichtingen uit artikel 13.3 heeft voldaan als daarom wordt gevraagd.

ARTIKEL 14 TOEPASSELIJK RECHT, GESCHILLENBESLECHTING EN RANGORDE

14.1 Op deze Verwerkersovereenkomst is Nederlands recht van toepassing.

14.2 Geschillen over deze Verwerkersovereenkomst worden voorgelegd aan de bevoegde rechter in de plaats waar Verwerkingsverantwoordelijke gevestigd is.

14.3 Als er tegenstrijdigheden zijn tussen deze Verwerkersovereenkomst en de Overeenkomst voor wat betreft de Verwerking van Persoonsgegevens, gelden de bepalingen van deze Verwerkersovereenkomst.

ALDUS OVEREENGEKOMEN DOOR PARTIJEN:

[NAAM VERWERKINGSVERANTWOORDELIJKE ……..]	**[NAAM VERWERKER……]**
_____/_____/_____	_____/_____/_____
Datum	*Datum*
_____	_____

Naam

_____

Handtekening

Naam

_____

Handtekening

Bijlage A: Specificatie van de Verwerking van de Persoonsgegevens

Omschrijving verwerking ('wat ga je doen')	**Doel van de verwerking ('waarom ga je dit doen')**	**Betrokkenen**	**Persoons-gegevens**	**Bewaartermijn(en) van de Persoonsgegevens**
1 ….				
2 ….				
3 ….				

De door Verwerker ingeschakelde Subverwerkers zijn:

Subverwerker (naam incl. plaats van vestiging)	**Persoonsgegevens die Subverwerker verwerkt**	**Omschrijving van de reden voor de subverwerking**	**Land van verwerking en relevant doorgifte-instrument**

De doorgiften naar derde landen bij de Verwerking zijn:

Doorgifte naar derde landen (naam partij + welk derde land)	**Doel doorgifte (kostenbesparingen, schaalvoordelen of beveiligingsverbeteringen)**	**Doorgifte-instrument**	**Aanvullende maatregelen naar aanleiding van een doorgifte aan een derde land (indien van toepassing)**

Contactgegevens:

Algemene contactgegevens	Naam	Functie	E-mailadres	Telefoonnummer
Verwerkingsverantwoordelijke				
Verwerker				

Datum bijlage: [DATUM…….]

Bijlage B: Beveiligingsmaatregelen

Instructies:
***Verwerker* heeft meerdere opties om aan te tonen welke passende maatregelen er zijn getroffen, om gegevens binnen deze Verwerking te beschermen.**

Kies voor de eigen maatregelen (in volgorde van voorkeur) ten minste één van onderstaande vier opties, om aan te tonen dat passende maatregelen zijn getroffen ter bescherming van gegevens. Vul binnen deze optie de tabel aan.

Wordt in Bijlage-A één of meerdere Subverwerker genoemd, dan dient Verwerker voor elke Subverwerker te kunnen aantonen, hoe passende maatregelen zijn getroffen die van hetzelfde (of hoger) niveau zijn als de bescherming die *Verwerker* zelf biedt. De primaire controletaak ligt bij de Verwerker en de verantwoordelijkheid voor toezicht op de uitvoer van deze controletaak bij de HAN als Verwerkingsverantwoordelijke. Gebruik hiervoor de tabel in Bijlage-A.

☐ Optie #1: ISO27001-certificering

Er wordt voldaan aan de actuele versie van de ISO/IEC-27001. Hiervoor kan *Verwerker* naar een publieke pagina verwijzen of het ISO27001-certificaat digitaal aanleveren als bijlage, inclusief de op het certificaat genoemde versie Statement of Applicability (SoA), ofwel Verklaring van Toepasselijkheid (VvT):

☐ Standaard	ISO/IEC 27001	2022	
☐ Weblocatie **☐ Bijlage**	https:// #		
Scope			
Geldig vanaf			
Geldig tot			
SoA/VvT	Versie		
☐ Weblocatie **☐ Bijlage**	https:// #		

De scope van de certificering betreft alle systemen, data, personen en middelen die op deze *Verwerking* van toepassing zijn.

Alle controls uit de ISO27002 zijn toegepast.

of

Er is een duidelijke en valide reden beschreven, waarom desbetreffende control uit-scope is genomen.

Verwerker heeft minimaal één interne audit-cyclus met positief resultaat doorlopen.

Waar mogelijk is Verwerker (extra) gecertificeerd tegen de:
- ISO/IEC-27701, voor Privacymanagement.

- ISO/IEC-27017, bij het gebruik van clouddiensten.

Hiervoor levert Verwerker het volgende bewijs aan:

☐ **Standaard**	ISO/IEC 27701	2019	
☐ **Weblocatie** ☐ **Bijlage**	https:// #		
Geldig vanaf			
Geldig tot			
☐ **Standaard**	ISO/IEC 27017	2015	
☐ **Weblocatie** ☐ **Bijlage**	https:// #		
Geldig vanaf			
Geldig tot			

Verwerker verleent conform Artikel 8 op verzoek van *Verwerkingsverantwoordelijke* inzage in de (samenvatting) rapportage met bevindingen van de onafhankelijke auditor en bij aanwezigheid van de tussentijdse cyclus audit, de meest recente rapportage van de interne auditor.

Contactpersoon	

☐ **Optie #2: Vergelijkbare certificering of accreditatie**

Verwerker voldoet aan een vergelijkbare actuele certificering of accreditering die, zoals de ISO27001, in voldoende mate de borging van informatiebeveiliging kan aantonen.

Voorbeelden zijn: Service Organization Control (SOC) 2 Type-II, International Standard on Assurance Engagements (ISAE) 3402 Type 2, Baseline Informatiebeveiliging Overheid (BIO) of de NEN7510 voor informatiebeveiliging in de zorgsector.

Hiervoor levert *Verwerker* het volgende bewijs aan:

☐ **Standaard**			
☐ **Weblocatie** ☐ **Bijlage**	https:// #		
Geldig vanaf			
Geldig tot			

Er wordt tijdens de betreffende audit op effectiviteit getoetst tegen de opzet, bestaan & werking.

Verwerker voert een onafhankelijke audit uit door een geaccrediteerde auditpartij, voorzien van een ondertekende “verklaring van zekerheid”.

Het audit-assurancerapport is conform artikel 8 op verzoek inzichtelijk voor *Verwerkingsverantwoordelijke*.

of

Verwerker verleent conform artikel 8 het recht-tot-auditen aan *Verwerkingsverantwoordelijke,* welke op verzoek kan worden ingezet

Contactpersoon	

☐ **Optie #3: STAR CIAQ**
Verwerker levert een transparante en gestandaardiseerde lijst van maatregelen aan, op basis van de meest recente versie van door de Cloud Security Alliance (CSA) ontwikkelde: Consensus Assessments Initiative Questionnaire (CIAQ).

Verwerker kan hiervoor verwijzen naar een publieke pagina, de CSA STAR Registry vermelding of de ingevulde vragenlijst digitaal bijvoegen als bijlage.

☐ **Weblocatie**	https://
☐ **Registry vermelding**	https://cloudsecurityalliance.org/star/registry/
☐ **Zie bijlage**	#

☐ **Optie #4: Maatregelenlijst**
Verwerker specificeert in onderstaande tabel verwijzing naar door topmanagement goedgekeurde documenten, middels beleidsnamen en waar nodig paginanummers, waar beschreven staat welke passende maatregelen er zijn genomen voor alle middelen die worden ingezet voor deze Verwerking.

Verwerker toetst periodiek en minimaal eens per jaar de effectiviteit van desbetreffende maatregelen op opzet, bestaan én werking.

Verwerker verleent conform artikel 8 op verzoek van *Verwerkingsverantwoordelijke* inzage in de genoemde pagina's en beleidsdocumenten.

Contactpersoon	

#	Onderwerp	Maatregel	Toelichting
1	Informatie-beveiligings- en privacybeleid	Verwerker heeft een informatiebeveiligings- en privacybeleid dat voldoet aan de AVG en eventuele richtsnoeren van de Autoriteit Persoonsgegevens en aansluit op algemene standaarden zoals ISO 27001/2/18, NOREA of CoBIT. Verwerker heeft dit beleid intern gecommuniceerd en concreet geïmplementeerd door middel van gedocumenteerde procedures.	

#	Onderwerp	Maatregel	Toelichting
2	Versleutelde opslag en verzending gegevens	Verwerker past actuele en algemeen als veilig beschouwde vormen van versleuteling (encryptie) toe op gegevens voor opslag (‘at rest’) en verzending (‘in transit’) om het risico te minimaliseren dat de inhoud van de gegevens kan worden ingezien door personen die daar niet toe bevoegd zijn.	
3	Access management	Verwerker past de principes van ‘least privilege’ en ‘need-to-know’ toe op zijn medewerkers en toegestane Subverwerkers. Verwerker zal tijdig gebruikerstoegang intrekken of wijzigen bij enige verandering in de status van zijn of Subverwerkers’ medewerkers Verwerker maakt gebruik van actuele en algemeen als veilig beschouwde vormen van versleuteling (encryptie) ten behoeve van identificatie, authenticatie en autorisatie.	
4	Medewerkers	Verwerker informeert zijn medewerkers over hun verantwoordelijkheden m.b.t. informatiebeveiliging en ziet erop toe dat medewerkers hun verplichtingen nakomen.	
5	Contract-management subverwerkers	Verwerker sluit met iedere toegestane Subverwerker een schriftelijke overeenkomst die de Subverwerker contractueel verplicht tot nakoming van dezelfde verplichtingen in verband met de Verwerking als die waar Verwerker op grond van deze Verwerkersovereenkomst aan is gebonden. Verwerker ziet er nauwlettend op toe dat Subverwerkers hun verplichtingen nakomen.	
6	Security incident detection & response	Verwerker heeft gedocumenteerd beleid dat geschikt is om Inbreuken te detecteren, op te lossen en te melden.	
7	Vulnerability / patch management	Verwerker zoekt regelmatig of doorlopend naar kwetsbaarheden binnen de gebruikte en aangeboden applicaties, systemen en netwerken. Verwerker installeert, implementeert security patches direct of zo snel mogelijk na het verschijnen daarvan.	

#	Onderwerp	Maatregel	Toelichting
8	Netwerk- en systeem-beveiliging	Verwerker heeft maatregelen getroffen om misbruik van en malware op het netwerk en de systemen van Verwerker tegen te gaan en te detecteren (zoals firewalls en antivirussoftware van betrouwbare leveranciers).	
9	Fysieke toegangs-beveiliging	Verwerker neemt passende maatregelen (zoals sloten, camera's, alarmsystemen) om de ruimtes waarin gegevens kunnen worden verwerkt, te beveiligen tegen onbevoegde toegang.	
10	Logging en monitoring	Door logging en monitoring wordt aangetoond dat slechts legitieme gebruikers en/of toepassingen de gegevens gebruiken. Bij signalering van niet-legitieme gebruikers en/of toepassingen wordt passende actie ondernomen.	
11	Locatie aantonen	Verwerker kan de fysieke locatie/geografie van opgeslagen gegevens aantonen.	
12	Business continuity & disaster recovery	Verwerker heeft beleid, procedures en processen geïmplementeerd om te waarborgen dat de geleverde diensten of producten en de verwerkte gegevens beschikbaar blijven in geval van onvoorziene omstandigheden en rampen, dan wel zo snel mogelijk volledig worden hersteld.	
13	Veilige applicatie-ontwikkeling	Verwerker gebruikt industriestandaarden (bv. OWASP, BSIMM, ACS, NIST) om beveiliging in applicatieontwikkeling te integreren.	
14	Onafhankelijke controle	Verwerker staat toe dat een externe partij audits, kwetsbaarheidsscans en periodieke penetratietests op zijn applicaties en netwerken uitvoert in opdracht van Verwerkingsverantwoordelijke, in overleg met Verwerker. Bij voorkeur geeft Verwerker zelf ook regelmatig opdracht aan deskundige externe partijen om audits, kwetsbaarheidsscans en periodieke penetratietests op zijn applicaties en netwerken uit te voeren.	

#	Onderwerp	Maatregel	Toelichting
		Bij voorkeur heeft Verwerker ook beleid en procedures voor het vinden en melden van beveiligingsproblemen door onafhankelijke beveiligingsonderzoekers (zoals *responsible disclosure policy* en/of *bug bounty programma*). Het toekennen van beloningen aan partijen die substantiële beveiligingsproblemen op een verantwoorde manier hebben gemeld, wordt hierbij als positief beschouwd.	

Bron: SURF model verwerkersovereenkomst versie 4.0 NL

15	Back-up en herstel	Verwerker zorgt ervoor dat periodiek back-ups worden gemaakt om gegevens te beschermen tegen verlies door verstoringen of incidenten. De back-up gegevens worden veilig opgeslagen conform back-up & herstelbeleid en dataretentie beleid. Herstelprocedures zijn gedocumenteerd en worden periodiek getest. De hersteltijden voldoen aan de gestelde afspraken omtrent hersteltijden (RTO) en acceptabel dataverlies (RPO).	

Bron: HAN Control Framework (HCF)

Bijlage C: Melden Inbreuk

Voor het melden van een Inbreuk kan contact worden opgenomen met:

Contactgegevens bij Inbreuk	**Naam**	**Functie**	**E-mail adres**
Verwerkings-verantwoordelijke	Informatiebeveiligings- en privacyteam	Privacy Officers en ISO's	Privacy@han.nl
Verwerker			

Verwerker vermeldt bij het melden van een Inbreuk in ieder geval de informatie zoals beschreven in de meest recente versie van het 'Meldloket datalekken' van de Autoriteit Persoonsgegevens, te vinden op: https://datalekken.autoriteitpersoonsgegevens.nl/, uitgewerkt in de 'Vragenlijst meldformulier datalekken': https://autoriteitpersoonsgegevens.nl/documenten/vragenlijst-meldformulier-datalekken.

Datum van de laatste wijziging: [DATUM…..]