Tilburg University Model Verwerkersovereenkomst

Versie: 3.2

Datum: maart 2025

Vul alle gele highlights in voorafgaand aan het ondertekenen van deze overeenkomst.

Gebaseerd op SURF Model Verwerkersovereenkomst 4.0, SURF Juridisch Normenkader (Cloud)services.

DE ONDERGETEKENDEN:

- **Tilburg University**[1]**,** gevestigd aan de Warandelaan 2 te Tilburg, Kamer van Koophandel nummer 41095855 en rechtsgeldig vertegenwoordigd door **[VERTEGENWOORDIGER]** (hierna: **"Verwerkingsverantwoordelijke"**);

- **[NAAM LEVERANCIER/VERWERKER],** gevestigd aan het [ADRES] te [PLAATS], Kamer van Koophandel nummer [KVK] 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 gesloten met kenmerk <KENMERK VAN DE OVEREENKOMST> 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 de 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 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

[1] Tilburg University gaat uit van de Stichting Katholieke Universiteit Brabant.

(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 11.3 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. Het oordeel over de technische en organisatorische maatregelen die Verwerker heeft geïmplementeerd, is opgenomen in Bijlage B.

6.2 Ten bewijze van het voldoen aan de gestelde technische en organisatorische beveiligingsmaatregelen dient Verwerker de door Tilburg University intern opgestelde Procedure Security Check te doorlopen. Het oordeel van de toetsing wordt vastgelegd in Bijlage B.

6.3 Bij de beoordeling van het passende beveiligingsniveau houdt Verwerker rekening 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, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.

6.4 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 binnen 24 uur na ontdekking van de Inbreuk. Verwerker informeert Verwerkingsverantwoordelijke via de contactpersonen en de contactgegevens van Verwerkingsverantwoordelijke zoals opgenomen in Bijlage A en ten minste ten aanzien van alle informatie zoals die blijkt uit het meest recente formulier datalekken van de Autoriteit Persoonsgegevens, welke te vinden is op de website van de Autoriteit Persoonsgegevens. Verwerker garandeert dat de verstrekte informatie, voor zover bekend bij Verwerker op dat moment, volledig, correct en accuraat is. 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 A 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 is verplicht conform artikel 8.2 periodiek door een extern deskundige een onafhankelijke audit te laten uitvoeren ten aanzien van de organisatie van Verwerker, teneinde aan te tonen dat Verwerker voldoet aan het bepaalde in de Overeenkomst, de Verwerkersovereenkomst, de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens.

8.2 Verwerkingsverantwoordelijke legt de frequentie van de door Verwerker uit te voeren periodieke audit, zoals bedoeld in artikel 8.1, vast in Bijlage A.

8.2.1 Verwerker verricht tenminste eenmaal per twee jaar een periodieke audit, zoals bedoeld in artikel 8.1, tenzij artikel 8.2.2 of 8.2.3 van toepassing is.

8.2.2 Indien Bijzondere categorieën Persoonsgegevens worden verwerkt of een Verwerking wordt verricht die een hoog risico inhoudt voor de rechten en vrijheden van de Betrokkenen, verricht Verwerker tenminste eenmaal per jaar een periodieke audit, zoals bedoeld in artikel 8.1.

8.2.3 Indien Verwerker uitsluitend verwerkingen verricht die een laag risico inhouden voor de rechten en vrijheden van Betrokkenen, is Verwerker niet gehouden tot het verrichten van een periodieke audit, zoals bedoeld in artikel 8.1. Verwerkingsverantwoordelijke stelt vast of er sprake is van een laag risico.

8.3 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.

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

8.5 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.

8.6 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 11.3 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. AANSPRAKELIJKHEID

10.1 Een Partij kan geen beroep doen op een aansprakelijkheidsbeperking, die is opgenomen in de Overeenkomst of andere tussen Partijen bestaande overeenkomst of regeling, ten aanzien van een door de andere Partij ingestelde:

a) verhaalsactie op grond van artikel 82 AVG; of

b) schadevergoedingsactie uit hoofde van de Verwerkersovereenkomst, indien en voor zover de actie bestaat uit verhaal van een aan de Toezichthoudende autoriteit betaalde geldboete die geheel of gedeeltelijk toerekenbaar is aan de andere Partij.

Het bepaalde in dit artikel laat onverlet de rechtsmiddelen die de aangesproken Partij op grond van de geldende wet- of regelgeving ter beschikking staat.

10.2 Iedere Partij is verplicht de andere Partij zonder onnodige vertraging op de hoogte te stellen van een (mogelijke) aansprakelijkstelling of het (mogelijk) opleggen van een boete door de Toezichthoudende autoriteit, beiden in verband met de Verwerkersovereenkomst. Iedere Partij is in redelijkheid verplicht de andere Partij informatie te verstrekken en/of ondersteuning te verlenen ten behoeve van het voeren van verweer tegen een (mogelijke) aansprakelijkstelling of boete, zoals bedoeld in de vorige volzin. De Partij die informatie verstrekt en/of ondersteuning verleent, is gerechtigd om eventuele redelijke kosten dienaangaande in rekening te brengen bij de andere Partij, Partijen informeren elkaar zo veel mogelijk vooraf over deze kosten.

ARTIKEL 11. WIJZIGING

11.1 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.

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

11.3 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.

11.4 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 12. DUUR EN BEËINDIGING

12.1 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.

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

12.3 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 aangegeven door Verwerkingsverantwoordelijke, 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.

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

12.5 Verwerker bevestigt schriftelijk aan Verwerkingsverantwoordelijke dat hij aan alle verplichtingen uit artikel 12.3 heeft voldaan als daarom wordt gevraagd.

ARTIKEL 13. TOEPASSELIJK RECHT EN GESCHILLENBESLECHTING

13.1 Op deze Verwerkersovereenkomst is hetzelfde recht van toepassing als dat van de Overeenkomst.

13.2 Geschillen over deze Verwerkersovereenkomst worden voorgelegd aan de bevoegde rechter van de Overeenkomst.

13.3 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:

Tilburg University	**[NAAM VERWERKER]**
<datum invullen>	<datum invullen>
<naam invullen>	<naam invullen>
_____	_____
Handtekening	*Handtekening*

Bijlage A: Specificatie van de Verwerking van Persoonsgegevens

Versienummer XX, Datum laatste aanpassing: XX-XX-XX

NB. Indien Verwerker meerdere (optionele) Diensten aanbiedt aan Verwerkingsverantwoordelijke, is het mogelijk de informatie op te nemen in separate Bijlage(n), die als volgt genummerd worden: "Bijlage A1", "Bijlage A2", etc.
Deze Bijlagen dienen aan de Verwerkersovereenkomst te worden gehecht.

Omschrijving verwerking ('wat ga je doen')	**Doel van de verwerking ('waarom ga je dit doen')**	**Betrokkenen**	**(Categorieën) persoons-gegevens[2]**	**Bewaartermijn(en) en Vernietiging van de Persoonsgegevens**
In te vullen door Verwerkingsverantwoordelijke				
1 ….				
2 ….				
3 ….				

Risicoklasse (conform de Vertrouwelijkheid uit de BIV-classificatie)
Laag: publieke persoonsgegevens (bv. zakelijk e-mailadres op internet) *Midden: niet publieke, maar ook geen bijzondere categorieën persoonsgegevens (bv. inschrijving van een student)* *Hoog: bijzondere categorieën persoonsgegevens* *In te vullen door Verwerkingsverantwoordelijke*

Frequentie verrichten van audit en motivering indien geen verplichting (artikel 8.1 t/m 8.2.3)
In te vullen door Verwerkingsverantwoordelijke

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**
In te vullen door Verwerker			

[2] Gebruikersgegevens mag Verwerker niet verwerken, tenzij deze gegevens geanonimiseerd zijn.

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)**
In te vullen door Verwerker			

Contactgegevens:

Algemene contactgegevens	**Naam**	**Functie**	**E-mailadres**	**Telefoon nummer**
Verwerkingsverantwoordelijke				
Algemene contactpersoon (proceseigenaar)	...	...	...	...
Functionaris Gegevensbescherming	M.R.G. Herregodts	FG	fg@tilburguniversity.edu	+31 13 466 3359
Bij melden van een inbreuk				
Algemene contactpersoon (proceseigenaar)	...	...	...	...
Functionaris Gegevensbescherming/ CISO Office	M.R.G. Herregodts/ CISO Office	FG PO ISO	datalek@tilburguniversity.edu	x
Bij spoed buiten kantoortijden ook naar: Computer Emergency Response Team (CERT)	CERT	CERT	cert@tilburguniversity.edu	x
Verwerker				
Algemene contactpersoon	…	…	…	…
Functionaris Gegevensbescherming	…	…	…	…

Bijlage B: Beveiligingsmaatregelen

Versienummer XX, Datum laatste aanpassing: XX-XX-XX

Voor de toetsing op de technische en organisatorische beveiligingsmaatregelen wordt de interne Procedure Security Check gevolgd. Het oordeel van de toetsing wordt vastgelegd in deze bijlage onder a.

Het CISO Office beoordeelt de beveiligingsmaatregelen en heeft hiervoor nodig:
- BIV-classificatie
- ISO 27001 certificering
- Verklaring van Toepasselijkheid op de ISO 27001 certificering

Of
- Een door de leverancier ingevuld SURF normenkader als er geen ISO certificaat is.

Het IT Security Office heeft hiervoor nodig:
- Pentest rapport (uitgevoerd door een gerenommeerd IT-security bedrijf, eventueel onder een Non Disclosure Agreement) - Dit is verplicht wanneer de BIV-classificatie midden of hoog scoort op integriteit en/of vertrouwelijkheid. Pentest mag niet ouder zijn dan één jaar.

Of
- STITCH - Mocht de BIV-classificatie laag scoren en er is geen pentest rapport, dan mag er een door de Verwerker een ingevuld STITCH-formulier worden aangeleverd.

a. Beoordeling toetsing beveiligingsmaatregelen

Beoordeling (kleurcode):

b. SURFconext-koppeling

Credentials (gebruikersnaam en wachtwoord) in (web) applicaties worden uitsluitend versleuteld verstuurd of ontvangen. Uitgangspunt is dat gebruik gemaakt wordt van SURFconext (wat voorziet in een Single Sign On (SSO) omgeving), tenzij dit onmogelijk is, dan wel niet proportioneel. Verwerker slaat de credentials van Verwerkingsverantwoordelijke niet op.

Maakt Verwerker gebruik van SSO omgeving van Verwerkingsverantwoordelijke? *(in te vullen door Verwerker)*
Ja/Nee
Indien Nee, motiveer waarom niet:

Onderhoud, duur en hardheid

De beveiligingseisen gelden doorlopend, zolang de software gebruikt wordt. Verwerker draagt actief zorg dat (nieuwe) kwetsbaarheden binnen redelijke termijn verholpen worden. CERT is het Computer Emergency Response Team van Verwerkingsverantwoordelijke en controleert periodiek op kwetsbaarheden en de SSL-configuratie van de gebruikte software en/of dienst.

<u>Bijlage C</u>: Aanpassingen t.o.v. standaard tekst << OPTIONEEL >>

Bij voorkeur wordt de gehele tekst van de modelovereenkomst gehandhaafd, uitgezonderd Bijlagen A en B, die per overeenkomst specifiek moeten worden ingevuld.
Mochten er toch additionele wijzigingen in de tekst nodig zijn (na onderhandelingen tussen Verwerkingsverantwoordelijke en Verwerker), dan kunnen de aanpassingen in deze Bijlage beschreven worden onder opgave van

- Artikelnummer,
- Betreffende tekst uit de standaard die vervalt
- Nieuwe vervangende tekst
- Reden van wijziging (bijv. n.v.t., eis niet acceptabel voor Verwerker, onderhandeld, etc.)

Art.	**Tekst die vervalt**	**Vervangende tekst**	**Reden**