PARTIJEN:

(1) **Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek TNO**, een publiekrechtelijke rechtspersoon op basis van artikel 3 van de TNO-wet, thans kantoorhoudende aan het Anna van Buerenplein 1, 2595 DA te Den Haag, ingeschreven in het handelsregister van de Kamer van Koophandel onder nummer 27376655, hierna te noemen '**Verwerkingsverantwoordelijke**, te dezen rechtsgeldig vertegenwoordigd door haar Raad van Bestuur, namens deze, [_____];

en

(2) [**NAAM VERWERKER**], een [besloten vennootschap / naamloze vennootschap / stichting / vereniging] statutair gevestigd te [PLAATS], ingeschreven in het handelsregister van de Kamer van Koophandel onder nummer [NUMMER], hierna te noemen **'Verwerker',** te dezen rechtsgeldig vertegenwoordigd door [_____], namens deze, [_____];

Verantwoordelijke en Verwerker worden gezamenlijk ook aangeduid als "**Partijen**" en elk afzonderlijk tevens een "**Partij**"

OVERWEGINGEN

A. Verantwoordelijke en Verwerker hebben op [DATUM] een Hoofdovereenkomst gesloten inzake 'vernieuwing en beheer website TNO'. De dienstverlening die Verwerker voor Verantwoordelijke uitvoert, richt zich primair op het verwerken van Persoonsgegevens zodat Verwerker namens en ten behoeve van Verantwoordelijke Persoonsgegevens verwerkt.

B. De verwerking van Persoonsgegevens onder de Hoofdovereenkomst houdt in dat Verwerker Persoonsgegevens : verzamelt, vastlegt, opslaat, bijwerkt of wijzigt, opvraagt, gebruikt, verstrekt door middel van doorzending, afschermt, wist of vernietigt.

C. Op grond van de Algemene Verordening Gegevensbescherming (AVG) zijn partijen verplicht om met elkaar een Verwerkersovereenkomst te sluiten om ervoor te zorgen dat Persoonsgegevens adequaat beschermd worden en de rechten van de betrokkenen adequaat zijn gewaarborgd. De Verantwoordelijke sluit deze Verwerkersovereenkomst met Verwerker om aan haar verplichtingen op grond van de AVG te voldoen en ervoor te zorgen dat Persoonsgegevens door Verwerker in overeenstemming met de AVG worden verwerkt.

1. DEFINTIES

In deze Verwerkersovereenkomst worden een aantal termen met een beginhoofdletter gebruikt. De definitie van deze termen komt overeen met de definitie die wordt gehanteerd in de AVG of voor zover de term daarin niet is gedefinieerd zoals hieronder aangegeven.

"**AVG"**	Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van de Richtlijn 95/46/EG (Algemene Verordening Gegevensbescherming);
"Data Protection Impact Assessment"	betekent een instrument om het effect van de beoogde verwerkingsactiviteiten op de bescherming van Persoonsgegevens te beoordelen;
"Hoofdovereenkomst"	betekent de [NAAM HOOFDOVEREENKOMST], inclusief wijzigingen en aanvullende overeenkomsten, overeengekomen tussen de Verantwoordelijke en de Verwerker bedoeld in overweging A bij deze Verwerkersovereenkomst;
"Instructie" of "Geïnstrueerd"	betekent de schriftelijke instructie van Verantwoordelijke aan Verwerker om een specifieke handeling met persoonsgegevens te verrichten (inclusief maar niet gelimiteerd tot pseudonimiseren, blokken, wissen en beschikbaar stellen);
"Security Breach"	betekent iedere inbreuk op de beveiliging van Persoonsgegevens die leidt of kan leiden tot ongeautoriseerde toegang, verlies, verandering of openbaarmaking van Persoonsgegevens;
"**Sub Verwerker**"	betekent een Verwerker, zoals gedefinieerd in de AVG, die in opdracht van de Verwerker Persoonsgegevens zal Verwerken ten behoeve van de Verantwoordelijke;
"**Technische en Organisatorische Maatregelen"**	betekent de technische en organisatorische beveiligingsmaatregelen die Persoonsgegevens beveiligen tegen verlies, diefstal, misbruik, onbevoegde toegang, ongewenste openbaarmaking, ongeoorloofde wijziging en verstrekking of tegen enige andere vorm van onrechtmatige verwerking en die, rekening

	houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen, een passend beveiligingsniveau garanderen gelet op de risico's van de Verwerking van Persoonsgegevens.
"**Toepasselijke Wetgeving** "	betekent alle wetgeving, inclusief de Algemene Verordening Gegevensbescherming 2016/679 van 27 april 2016, betreffende de bescherming van Persoonsgegevens die van toepassing is op de Verwerking van Persoonsgegevens in verband met de activiteiten die uitgevoerd worden op grond van de Hoofdovereenkomst;
"Verantwoordelijke"	Betekent de verwerkingsverantwoordelijke zoals bedoeld in artikel 1, aanhef en onder 7 van de AVG;
"Verwerken" of "Verwerking"	betekent elke handeling of elk geheel van handelingen met betrekking tot Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procédés, waaronder in ieder geval het verzamelen, vastleggen, ordenen, structuren, opslaan, bijwerken of wijzigen, opvragen. Raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, aligneren of het combineren, met elkaar in verband brengen alsmede het afschermen, wissen of vernietigen van gegevens;
"Verwerkersovereenkomst"	betekent deze verwerkersovereenkomst, inclusief eventuele bijlagen.

2. VERPLICHTINGEN VAN DE VERWERKER

2.1. De Verwerker zal:

a. Persoonsgegevens uitsluitend Verwerken onder de (uiteindelijke) verantwoordelijkheid van Verantwoordelijke in overeenstemming met de schriftelijke Instructies van Verantwoordelijke en op de wijze beschreven in Bijlage 1, waarbij de Verantwoordelijke de schriftelijke Instructies op elk moment kan wijzigen of intrekken;

b. Persoonsgegevens alleen bewaren zolang de Verantwoordelijke dat verlangt en de Persoonsgegevens wijzigen, anonimiseren, blokken of verwijderen zodra de Verantwoordelijke daartoe Instructies geeft;

c. ervoor zorgen dat alleen (i) haar werknemers; en (ii) Sub Verwerkers toegang krijgen tot Persoonsgegevens en slechts zolang dit noodzakelijk is in het kader van de uitvoering van de verplichtingen van de Verwerker onder de Hoofdvereenkomst;
d. de Verantwoordelijke informeren over de onmogelijkheid om een Instructie van Verantwoordelijke uit te voeren omdat de Instructie vermoedelijk niet in overeenstemming is met de Toepasselijke Wetgeving.

3. TECHNISCHE EN ORGANISATORISCHE MAATREGELEN

3.1. De Verwerker zal Technische en Organisatorische Maatregelen, zoals beschreven in Annex 2, treffen, in stand houden en zo nodig aanpassen om de Persoonsgegevens te beveiligen om een Security Breach te voorkomen.

3.2. De Verwerker staat er voor in dat de in artikel 3.1 genoemde Technische en Organisatorische Maatregelen:
a. adequaat en passend zijn voor de Verwerking rekening houdend met de aard van de Persoonsgegevens, de stand van de techniek, de kosten van de tenuitvoerlegging, 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; en
b. dusdanig worden vastgesteld en toegepast dat de Verantwoordelijke steeds in overeenstemming handelt met Toepasselijke Wetgeving op het gebied van Persoonsgegevens.

4. DOORGIFTE VAN PERSOONSGEGEVENS

4.1. De Verwerker mag geen Persoonsgegevens doorgeven en Verwerken in een land buiten de Europese Economische Ruimte (EER), tenzij de Verantwoordelijke voorafgaand aan de doorgifte schriftelijk Instructie geeft en:

a. dat land een passend beschermingsniveau biedt door middel van de eigen nationale wetgeving of gebonden is aan internationale verdragen en dit niveau van bescherming is erkend door de Europese Commissie via een adequaatheidsbesluit;

b. gebruik wordt gemaakt van een modelcontract als bedoeld in artikel 26, vierde lid, van richtlijn nr. 95/46/EG tussen de Verantwoordelijke en de Verwerker of een Sub Verwerker totdat de Europese Commissie bij besluit heeft vastgesteld dat dit artikel is gewijzigd, vervangen of ingetrokken. In dat geval is het doorgeven en Verwerken in een land buiten de Europese Economische Ruimte (EER) op grond van dit artikel niet langer toegestaan, totdat Verantwoordelijke en Verwerker een alternatieve overeenkomst hebben vastgesteld.

4.2. De onder artikel 4.1.b genoemde overeenkomsten mogen geen afbreuk doen aan de rechten van de Verantwoordelijke onder deze Verwerkersovereenkomst.

4.3. Onverminderd het bepaalde in artikel 4.1, geeft de Verantwoordelijke hierbij instructie en een volmacht aan de Verwerker om, op naam van de Verantwoordelijke, de Sub Verwerker

Instructies te geven en de onder artikel 4.1.b genoemde overeenkomsten te sluiten indien Persoonsgegevens worden doorgestuurd naar een Sub Verwerker in een land buiten de EER.

4.4. In geval van een doorgifte als omschreven in artikel 4.1 accepteert de Verwerker elke wijziging van deze Verwerkersovereenkomst die noodzakelijk is voor de Verantwoordelijke om te voldoen aan de Toepasselijke Wetgeving.

5. AUDITS

5.1. Verantwoordelijke is te allen tijde gerechtigd een audit, waaronder inspectie uit te (laten) voeren naar de naleving door de Verwerker en haar Sub Verwerkers van deze Verwerkersovereenkomst en meer specifiek naar de Technische en Organisatorische Maatregelen.

5.2 Een audit kan worden uitgevoerd door een door de Verantwoordelijke aangewezen onafhankelijke derde, die in dit opzicht verplicht is tot geheimhouding en die niet eerder begint dan twee weken nadat de Verantwoordelijke Verwerker hiervan op de hoogte heeft gesteld. Elke dergelijke audit volgt de redelijke beveiligingsvereisten van de Verwerker en zal niet onredelijk interfereren met de bedrijfsactiviteiten van de Verwerker.

5.2. De Verwerker en haar Sub Verwerkers zullen de Verantwoordelijke en haar auditors met betrekking tot een audit voorzien van redelijke medewerking, toegang tot de faciliteiten waar Persoonsgegevens Verwerkt worden en in elk geval alle informatie verschaffen die nodig is om de nakoming van de verplichtingen van Verwerker en de Sub Verwerkers onder de Verwerkersovereenkomst aan te tonen.

5.3 De bevindingen uit de uitgevoerde audit zullen door Partijen worden besproken en geëvalueerd, waarna de te treffen maatregelen die uit de bevindingen voortvloeien, voor zover van toepassing, door Partijen afzonderlijk dan wel gezamenlijk worden geïmplementeerd.

5.4 De kosten van de audit zijn voor Verantwoordelijke tenzij uit de audit blijkt dat Verwerker in strijd met deze Verwerkersovereenkomst handelt of heeft gehandeld.

6 SUB VERWERKERS

6.1 Het is Verwerker niet toegestaan Persoonsgegevens te doen Verwerken door Sub Verwerkers tenzij:

a. Verantwoordelijke voorafgaand aan de inschakeling van de desbetreffende Sub Verwerker, deze Sub Verwerker schriftelijk heeft goedgekeurd; en

b. Verwerker met de desbetreffende Sub Verwerker een schriftelijke overeenkomst heeft gesloten waarin deze Sub Verwerker verplichtingen overeenkomstig aan deze Verwerkersovereenkomst oplegt.

6.2 Verantwoordelijke mag aan haar goedkeuring van artikel 6.1 (A) voorwaarden verbinden.

7 GEHEIMHOUDING

7.1 Verwerker zal de Persoonsgegevens geheimhouden en zal haar werknemers, Sub Verwerkers en werknemers van Sub Verwerkers, voordat zij toegang verkrijgen tot de

Persoonsgegevens, contractueel verplichten tot geheimhouding van de Persoonsgegevens waarvan zij met betrekking tot de uitvoering van de Hoofdovereenkomst kennis kunnen nemen.

7.2 De geheimhoudingsplicht van Persoonsgegevens door Verwerker of Sub Verwerker kan alleen worden doorbroken wanneer:
- een wettelijk voorschrift verplicht om Persoonsgegevens te verstrekken; of
- de Verantwoordelijke instructie geeft tot verstrekking van de Persoonsgegevens.

8 AANSPRAKELIJKHEID

8.1 Verwerker vrijwaart en stelt schadeloos de Verantwoordelijke met betrekking tot de Verwerking van de Persoonsgegevens onder deze Verwerkersovereenkomst ter zake van (i) alle schade; en (ii) opgelegde boetes door de Toezichthoudende Autoriteit in verband met een toerekenbare tekortkoming van één of meer verplichtingen van de Verwerker onder deze Verwerkersovereenkomst.

9 BIJSTAND AAN VERANTWOORDELIJKE

9.1 Indien een Betrokkene bij de Verantwoordelijke een verzoek neerlegt tot onder meer:
- inzage van op hem betrekking hebbende Persoonsgegevens;
- rectificatie van op hem betrekking hebbende Persoonsgegevens;
- gegevenswissing (“recht op vergetelheid) van op hem betrekking hebbende Persoonsgegevens;
- beperking van de verwerking van op hem betrekking hebbende Persoonsgegevens;
- overdraagbaarheid van op hem betrekking hebbende Persoonsgegevens;

en dit verzoek een gerechtvaardigde uitoefening van een recht van Betrokkene onder de Toepasselijke Wetgeving betreft, zal Verwerker alle benodigde bijstand verlenen om de hieruit voortvloeiende verplichtingen van de Verantwoordelijke uit te voeren, waaronder het wissen, rectificeren en overdragen van Persoonsgegevens.

9.2 Indien Verantwoordelijke een Data Protection Impact Assessment dient uit te voeren voordat de Verwerker Persoonsgegevens (verder) kan Verwerken onder de Hoofdovereenkomst en daartoe bijstand van de Verwerker is vereist, zal de Verwerker daartoe de nodige bijstand verlenen.

10 MELDPLICHT

10.1 Verwerker zal Verantwoordelijke informeren over iedere Security Breach alsmede Verantwoordelijke informeren over:
a. het tijdstip van aanvang van de Security Breach;
b. de aard en de omvang van de Security Breach;
c. welke dienst en/of (ICT-)systeem bij de Security Breach betrokken is;
d. de verwachte hersteltijd;
e. aard en omvang van de betrokken databestanden en het aantal Betrokkenen;
f. de identiteit van Betrokkenen;
g. de mogelijke consequenties van de Security Breach voor de Betrokkenen alsmede een voorstel ter voorkoming van mogelijke schade en andere negatieve consequenties; en
h. welke maatregelen zijn genomen om de Security Breach te beëindigen.

10.2 Verwerker zal Verantwoordelijke onverwijld en in elk geval binnen **24 uur** na ontdekking van de Security Breach aan haar meldplicht conform artikel 10.1 voldoen en voorts Verantwoordelijke steeds volledig op de hoogte houden over de voortgang van het herstel en andere relevante ontwikkelingen aangaande de Security Breach en de gevolgen daarvan.

10.3 Verwerker zal onverwijld alle maatregelen nemen die redelijkerwijs van Verwerker kunnen worden verwacht om de nadelige gevolgen van de Security Breach in voorkomend geval te herstellen, dan wel zoveel mogelijk te beperken. Deze maatregelen zal de Verwerker voorts ook zo snel mogelijk aan de Verantwoordelijke melden.

10.4 Verwerker doet noch melding van de Security Breach aan de bevoegde nationale Toezichthoudende Autoriteit noch informeert Betrokkenen over de Security Breach. De Verantwoordelijke heeft de verantwoordelijkheid om de bevoegde nationale Toezichthoudende Autoriteit en Betrokkenen van de Security Breach op de hoogte te stellen conform artikel 33 van de AVG.

10.5 Verwerker rapporteert aan Verantwoordelijke in **januari van elk jaar** over opgetreden Security Breaches die in het voorgaande jaar hebben plaatsgevonden. Het rapport bevat een samenvatting van de opgetreden Security Breaches met de genomen maatregelen om Security Breach te beëindigen en om soortgelijke Security Breaches te voorkomen in de toekomst.

11 DUUR EN BEËINDIGING VERWERKERSOVEREENKOMST

11.1 Deze Verwerkersovereenkomst wordt gesloten op het moment dat Partijen deze hebben ondertekend en loopt door tot beëindiging van de Hoofdovereenkomst.

11.2 Verwerker draagt er zorg voor dat de hiervoor bedoelde Persoonsgegevens onverwijld na beëindiging van de Hoofdvereenkomst, of zoveel eerder als dat mogelijk is, op een wijze en met gebruik van een middel naar keuze van de Verantwoordelijke, worden overgedragen aan Verantwoordelijke.

11.3 Na overdracht, schriftelijke afwijzing van overdracht door Verantwoordelijke, of indien de Verantwoordelijke niet reageert, na één maand na het aanbod tot overdracht, dient de Verwerker de Persoonsgegevens onverwijld te vernietigen. Op eerste verzoek van Verantwoordelijke zal Verwerker schriftelijk bevestigen dat dit daadwerkelijk gebeurd is.

11.4 Na beëindiging van de Hoofdovereenkomst blijven de geheimhoudingsverplichtingen ten aanzien van Persoonsgegevens op grond van artikel 7 van deze Verwerkersovereenkomst onverminderd van kracht op Verwerker en eventueel door Verwerker ingeschakelde Sub verwerkers.

12 OVERIGE BEPALINGEN

12.1 Op deze Verwerkersovereenkomst is hetzelfde recht van toepassing als overeengekomen in de Hoofdovereenkomst.

12.2 Alle geschillen die naar aanleiding van deze Verwerkersovereenkomst of de uitvoering daarvan mochten ontstaan, zullen worden voorgelegd aan de bevoegde rechter zoals overeengekomen in de Hoofdovereenkomst.

12.3 Wijzigingen en aanvullingen van deze Verwerkersovereenkomst kunnen slechts schriftelijk, bij onderhandse akte ondertekend door beide partijen, worden overeengekomen.

12.4 In geval van enige inconsistentie tussen documenten en de bijlagen daarvan is de volgende volgorde van prioriteit van toepassing:

1. de Hoofdovereenkomst;
2. deze Verwerkersovereenkomst;
3. aanvullende voorwaarden en bepalingen, indien van toepassing.

Verantwoordelijke (TNO)	**Verwerker** [naam Partij]
Datum: ……..	Datum:……..
Plaats: ……..	Plaats:……..
Naam: ……..	Naam:……..
Handtekening: ……..	Handtekening:……..

ANNEX 1
BESCHRIJVING VERWERKING PERSOONSGEGEVENS

Categorieën van Betrokkenen

De categorieën van Betrokkenen van wie Persoonsgegevens worden verwerkt zijn: (bijv. klanten, onderzoekdeelnemers, minderjarigen, patiënten, werknemers)

- Websitegebruikers
- Nieuwsbriefabonnees
- Prospects
- Klanten
- Onderzoekdeelnemers
- Sollicitanten

Categorieën van Persoonsgegevens

De Persoonsgegevens die door Verwerker worden verwerkt zijn: (bijv. contactgegevens, audio/video, gezondheidsgegevens, BSN, financiële gegevens, IP-adressen, locatiegegevens):

- Naam
- Adres
- Woonplaats
- Email adres
- Geslacht M/V
- Geboortedatum
- Werkgever
- Functie
- Opleiding

Verwerking Persoonsgegevens

De Persoonsgegevens zullen door Verwerker als volgt worden verwerkt:

- Persoonsgegevens worden op diverse wijze verzameld, primair via de website door middel van een formulier dat gebruikers invullen. De verzamelde persoonsgegevens worden vastgelegd en opgeslagen in een speciaal daarvoor bedoelde (crm) applicatie. De vastgelegde persoonsgegevens in de applicatie kunnen worden beheerd, dat wil zeggen worden aangevuld, gewijzigd, gewist en vernietigd. De vastgelegde persoonsgegevens in de applicatie kunnen worden opgevraagd en gebruikt in andere gekoppelde applicaties zoals bijvoorbeeld maar niet uitsluitend de website, een HR applicatie, een Email applicatie.

ANNEX 2
DESCRIPTION OF TECHNICAL AND ORGANIZATIONAL MEASURES

Deze Annex beschrijft de Technische en Organisatorische Maatregelen en procedures die Verwerker zal nemen om de verwerking van Persoonsgegevens passend adequaat te beveiligen. Verwerker zal documentatie van de Technische en Organisatorische Maatregelen bewaren als bewijs. Deze maatregelen zorgen ervoor dat Persoonsgegevens worden beschermd tegen verlies, diefstal, misbruik, ongeoorloofde toegang, ongewenste wijziging en openbaarmaking of enige andere onrechtmatige verwerking. De Verantwoordelijke en de Verwerker hebben beoordeeld dat deze maatregelen passend zijn, daarbij rekening houdend met de aard, omvang, de context en de doeleinden van de verwerking evenals de waarschijnlijkheid dat deze risico's zich kunnen voordoen en de ernst van de gevolgen daarvan voor betrokkenen.

[BESCHRIJF HIERONDER DE TECHNISCHE EN ORGANISATORISCHE MAATREGELEN DIE DOOR VERWERKER WORDEN GENOMEN OM DE PERSOONSGEGEVENS TE BESCHERMEN TEGEN VERLIES, DIEFSTAL, MISBRUIK, ONGEAUTORISEERDE TOEGANG, ONGEWENSTE WIJZIGING EN OPENBAARMAKING VAN DE PERSOONSGEGEVENS]

Voorbeelden van Technische Maatregelen:

- *Maatregelen om de beschikbaarheid, integriteit en vertrouwelijkheid van de gegevens te borgen*
- *Maatregelen om de veerkracht van ICT-systemen te borgen*
- *Certificering bijv. ISO 27001*
- *Encryptie*
- *Pseudonimisering door middel van:*
    - *datamasking*
    - *shuffling*
    - *Look-up (vervanging van persoonsgegevens door andere gegevens)*
- *"Chinese muren' binnen systemen*
- *Logging van toegang tot de gegevens en verrichte verwerking*
- *Monitoring van logginggegevens*
- *Gebruikersnaam en wachtwoord*
- *Twee factor authenticatie*

Voorbeelden van Organisatorische Maatregelen:

- *Identiteits- en toegangsbeleid*
- *Toegangsbeleid ('need to know' basis)*
- *Extra beveiligde fysieke omgevingen*
- *Afgesloten kasten/ kluizen*
- *Fysieke toegangscontrole*
- *Screening van medewerkers*
    - *VOG*
    - *VGB*