(Datum: mei 2018)

Inhoud

Verwerkersovereenkomst ARVODI-2018

Contractnummer: [...].

De ondergetekenden:

1. De Staat der Nederlanden, waarvan de zetel is gevestigd te Den Haag, te dezen vertegenwoordigd door de Minister van Volksgezondheid, Welzijn en Sport, namens deze, de 5.1.2e van het Rijksinstituut voor Volksgezondheid en Milieu, namens deze 5.1.2e 5.1.2e Centrum Epidemiologie en Surveillance van Infectieziekten
hierna te noemen: Opdrachtgever,

en

2. **Julius Clinical Research B.V.**, (statutair) gevestigd te Broederplein 41-43 te (3703 CD) Zeist, te dezen vertegenwoordigd door 5.1.2e de heer 5.1.2e
hierna te noemen: Opdrachtnemer of Julius Clinical,

hierna gezamenlijk te noemen: Partijen;

OVERWEGENDE DAT:

- voor zover Opdrachtnemer Persoonsgegevens Verwerkt ten behoeve van Opdrachtgever in het kader van de Overeenkomst, Opdrachtgever krachtens artikel 4, onderdeel 7 en onderdeel 8, van de Verordening kwalificeert als verwerkingsverantwoordelijke voor de Verwerking van Persoonsgegevens en Opdrachtnemer als verwerker;
- Partijen in deze Verwerkersovereenkomst, zoals bedoeld in artikel 28, derde lid, van de Verordening, hun afspraken over de Verwerking van Persoonsgegevens door Opdrachtnemer wensen vast te leggen.

KOMEN OVEREEN:

Artikel 1. Begrippen

In deze Verwerkersovereenkomst wordt een aantal begrippen met een beginhoofdletter gebruikt. Aan deze begrippen komt de betekenis toe die hieraan wordt gegeven in artikel 1 van de Algemene Rijksvoorwaarden voor het verstrekken van opdrachten tot het verrichten van Diensten 2018 (ARVODI-2018). In afwijking daarvan of in aanvulling daarop wordt onder de volgende begrippen in deze Verwerkersovereenkomst verstaan:

1.1 Betrokkene: degene op wie een Persoonsgegeven betrekking heeft.

1.2 Inbreuk in verband met Persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

1.3 Overeenkomst: tussen Opdrachtgever en Opdrachtnemer Julius Clinical Overeenkomst inzake VASCO: A population-based prospective cohort study on vaccine effectiveness of COVID-19 vaccines in the Netherlands van March 3th 2021, met kenmerk NL76815.056.21.

1.4 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, die Opdrachtnemer in het kader van de Overeenkomst ten behoeve van Opdrachtgever verwerkt.

1.5 Verordening: 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).

1.6 Verwerkersovereenkomst: deze overeenkomst inclusief overwegingen en bijbehorende bijlagen.

1.7 Verwerking: een bewerking of een geheel van bewerkingen in het kader van de Overeenkomst met betrekking tot Persoonsgegevens, of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen.

Artikel 2. Voorwerp van deze Verwerkersovereenkomst

2.1 Deze Verwerkersovereenkomst regelt de Verwerking van Persoonsgegevens door Opdrachtnemer in het kader van de Overeenkomst.

2.2 De aard en het doel van de Verwerking, het soort Persoonsgegevens en de categorieën van Persoonsgegevens, Betrokkenen en ontvangers zijn in Bijlage 1 omschreven.

2.3 Opdrachtnemer zal passende technische en organisatorische maatregelen toepassen, opdat de Verwerking aan de vereisten van de Verordening voldoet en de bescherming van de rechten van de Betrokkene is gewaarborgd.

2.4 Opdrachtnemer zal voldoen aan de vereisten van de toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens.

Artikel 3. Inwerkingtreding en duur

3.1 Deze Verwerkersovereenkomst treedt in werking op het moment waarop deze door Partijen is ondertekend.

3.2 Deze Verwerkersovereenkomst eindigt nadat en voor zover Opdrachtnemer alle Persoonsgegevens overeenkomstig artikel 10 heeft gewist of terugbezorgd.

3.3 Geen van Partijen kan deze Verwerkersovereenkomst tussentijds opzeggen.

Artikel 4. Omvang verwerkingsbevoegdheid Opdrachtnemer

4.1 Opdrachtnemer Verwerkt de Persoonsgegevens uitsluitend in opdracht en op basis van schriftelijke instructies van Opdrachtgever behoudens afwijkende wettelijke voorschriften die op Opdrachtnemer van toepassing zijn.

4.2 Indien een instructie als bedoeld in het eerste lid naar het oordeel van Opdrachtnemer in strijd is met een wettelijk voorschrift inzake gegevensbescherming, stelt hij Opdrachtgever daarvan voorafgaand aan de Verwerking in kennis, tenzij een wettelijk voorschrift deze kennisgeving verbiedt.

4.3 Indien Opdrachtnemer op grond van een wettelijk voorschrift Persoonsgegevens dient te verstrekken, informeert hij Opdrachtgever zo snel als redelijkerwijs mogelijk, en zo mogelijk voorafgaand aan de verstrekking.

4.4 Opdrachtnemer heeft geen zeggenschap over het doel van en de middelen voor de Verwerking van Persoonsgegevens.

Artikel 5. Beveiliging van de Verwerking

5.1 In aanvulling op artikel 15 van de ARVODI-2018 en onverminderd artikel 2.3 treft Opdrachtnemer de technische en organisatorische beveiligingsmaatregelen zoals beschreven in Bijlage 2.

5.2 Partijen erkennen dat het waarborgen van een passend beveiligingsniveau voortdurend kan dwingen tot het treffen van aanvullende beveiligingsmaatregelen. Opdrachtnemer waarborgt een op het risico afgestemd beveiligingsniveau.

5.3 Indien en voor zover Opdrachtgever daarom uitdrukkelijk schriftelijk verzoekt, zal Opdrachtnemer aanvullende maatregelen treffen met het oog op de beveiliging van de Persoonsgegevens.

5.4 Opdrachtnemer Verwerkt Persoonsgegevens niet buiten de Europese Unie, tenzij hij daarvoor uitdrukkelijk schriftelijk toestemming heeft verkregen van Opdrachtgever en behoudens afwijkende wettelijke verplichtingen.

5.5 Opdrachtnemer informeert Opdrachtgever zonder onredelijke vertraging zodra hij kennis heeft genomen van onrechtmatige Verwerkingen van Persoonsgegevens of inbreuken op beveiligingsmaatregelen zoals genoemd in het eerste en tweede lid.

5.6 Rekening houdend met de aard van de verwerking en de hem ter beschikking staande informatie verleent Opdrachtnemer Opdrachtgever bijstand bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36 van de Verordening.

Artikel 6. Geheimhouding door Personeel van Opdrachtnemer

6.1 De Persoonsgegevens hebben een vertrouwelijk karakter als bedoeld in artikel 13.1 van de ARVODI-2018.

6.2 Opdrachtnemer toont op verzoek van Opdrachtgever aan dat zijn Personeel zich ertoe heeft verbonden vertrouwelijkheid in acht te nemen als bedoeld in artikel 13.2 van de ARVODI-2018.

Artikel 7. Subverwerker

Wanneer Opdrachtnemer, met inachtneming van het bepaalde in artikel 8 van de ARVODI-2018, een andere verwerker inschakelt om ten behoeve van Opdrachtgever verwerkingsactiviteiten te verrichten, worden aan deze andere verwerker bij een overeenkomst dezelfde verplichtingen inzake gegevensbescherming opgelegd als die welke in deze Verwerkersovereenkomst zijn opgenomen.

Artikel 8. Bijstand vanwege rechten van Betrokkene

Rekening houdend met de aard van de verwerking verleent Opdrachtnemer, door middel van passende technische en organisatorische maatregelen, Opdrachtgever bijstand, voor zover

mogelijk, bij het vervullen van diens plicht om verzoeken om uitoefening van de in hoofdstuk III van de Verordening vastgelegde rechten van de Betrokkene te beantwoorden.

Artikel 9. Inbreuk in verband met Persoonsgegevens

9.1 Opdrachtnemer informeert Opdrachtgever zonder onredelijke vertraging, zodra hij kennis heeft genomen van een Inbreuk in verband met Persoonsgegevens, overeenkomstig de afspraken zoals vastgelegd in Bijlage 3.

9.2 Opdrachtnemer informeert Opdrachtgever ook na een melding op grond van het eerste lid over ontwikkelingen betreffende de Inbreuk in verband met Persoonsgegevens.

9.3 Partijen dragen elk de door henzelf in verband met de melding aan de bevoegde toezichthoudende autoriteit en Betrokkene te maken kosten.

Artikel 10. Terugbezorgen of wissen Persoonsgegevens

10.1 Na afloop van de Overeenkomst draagt Opdrachtnemer, naar gelang de keuze van Opdrachtgever, zorg voor het terugbezorgen aan Opdrachtgever of het wissen van alle Persoonsgegevens. Opdrachtnemer verwijdert kopieën, behoudens afwijkende wettelijke voorschriften.

10.2 Persoonsgegevens worden in de door Opdrachtgever aangegeven vorm, op tussen Partijen vooraf overeengekomen kosten van de Opdrachtgever, en op de door Opdrachtgever aangegeven wijze terugbezorgd.

Artikel 11. Informatieverplichting en audit

11.1 Opdrachtnemer stelt alle informatie ter beschikking die redelijkerwijs nodig is om aan te tonen dat de verplichtingen uit deze Verwerkersovereenkomst zijn en worden nagekomen.

11.2 Opdrachtnemer verleent alle benodigde medewerking aan audits met betrekking tot artikel 11.1. Opdrachtgever zal Opdrachtnemer met een redelijke voorafgaande termijn informeren over een geplande audit en Opdrachtgever zal geheimhouding in acht nemen met betrekking tot informatie waarvan Opdrachtgever kennis krijgt naar aanleiding van een audit. Audits dienen plaats te vinden gedurende standaard kantoortijden en met zo min mogelijk verstoring van de werkzaamheden van Opdrachtnemer.

Aldus op de laatste van de twee hierna genoemde data overeengekomen en in tweevoud ondertekend,

Bilthoven, [28/04/2021] Zeist, [28/04/2021]

De minister van Volksgezondheid, Welzijn en Sport, namens deze, de 5.1.2e

5.1.2e van het RIVM, namens deze

5.1.2e

5.1.2e

5.1.2e

Julius Clinical Research B.V.

5.1.2e

5.1.2e

5.1.2e

Bijlage 1. De Verwerking van Persoonsgegevens

In deze bijlage moet in ieder geval het volgende worden gespecificeerd:

Het onderwerp/aard en doel van de Verwerking	
Het soort Persoonsgegevens	NAW - en bijzondere persoonsgegevens
Beschrijving categorieën Persoonsgegevens	Gewone persoonsgegevens: naam, adres, woonplaats, geboortedatum, emailadres en telefoonnummer. Bijzondere persoonsgegevens: Via vragenlijsten worden volgende gegevens verzameld. - Geslacht - Etniciteit - Opleiding - Beroep - Gezondheidsstatus - Bezoek/contact zorgverlener - Medicatie gebruik - SARS-CoV-2 infecties - Vaccinatie status - Gedrag aangaande de COVID-19 metingen
Beschrijving categorieën Betrokkenen	De deelnemers aan het onderzoek
Beschrijving categorieën ontvangers van Persoonsgegevens	Julius Clinical: verwerker MailStreet B.V.: verwerker – overeenkomst via Julius Clinical Daklapack: verwerker – overeenkomst via Julius Clinical Your research: verwerker – overeenkomst via Julius Clinical RIVM: verwerkingsverantwoordelijke

Voor de inhoud van deze bijlage kan onder meer gebruik worden gemaakt van de registratie die de Verwerkingsverantwoordelijke op grond van artikel 30 van de Verordening dient aan te houden.

Bijlage 2. Passende technische en organisatorische maatregelen

In deze bijlage moeten de normen en maatregelen die Opdrachtnemer in het kader van de beveiliging van de Verwerking moet hanteren respectievelijk treffen worden gespecificeerd. Hiervoor kan worden verwezen naar documenten waarin normen en maatregelen zijn vastgelegd, zoals in voorkomend geval het programma van eisen of de offerteaanvraag.

This 'Bijlage 2' includes certain details of the technical and organizational measures implemented by Julius Clinical (Opdrachtnemer) as required by Article 32(1) GDPR.

Julius Clinical's System Life Cycle Management standard operating procedure and System Management Plan describes the steps to be taken to maintain a compliant IT-environment on an infrastructure level and a business application level.

The following descriptions provide an overview of the technical and organisational security measures implemented. It should be noted however that, in some circumstances, in order to protect the integrity of the security measures and in the context of data security, detailed descriptions may not be available. It's acknowledged and agreed that the technical and organisational measures described therein and in our internal Security Policies will be updated and amended from time to time, at our sole discretion. Notwithstanding the foregoing, the technical and organisational measures will not fall short of those measures described in our IT Security Policy in any material, detrimental way.

Hosting Infrastructure
We utilise a mix of hosting infrastructure in the form of an on-premise data centre, and colocation and cloud services with vendors that maintain a current ISO 27001 certification.

We will not utilise cloud service providers that do not maintain the aforementioned certification, or other substantially similar or equivalent certifications and/or attestations.

Our on-premise and colocation hosting infrastructure is managed according to Julius Clinical's System Management Plan. The System Management Plan describes the activities that are performed to manage the Hosting Infrastructure including implemented Software during operational use and to maintain its qualified state. A subset of relevant activities will be described in the sections hereunder.

Physical Access Control
Technical or organisational measures regarding access control, especially regarding legitimation of authorised persons:

The aim of the entrance control is to prevent unauthorised people from physically accessing such data processing equipment which processes or uses Customer Data.

We employ measures designed to prevent unauthorized persons from gaining access to data processing systems.

For our colocation and cloud services vendors, the constructional and substantive security standards comply with the security requirements for data centres that maintain an ISO 27001 certification or other substantially similar or equivalent certifications and/or attestations.

Physical access to the Julius Clinical office and our on-premise data centre is secured through personal badges. Only properly authorized staff have access to the on-premise data centre and entry is controlled through logging and monitored through CCTV.

System Access Control
Technical and organisational measures regarding the user ID and authentication:

The aim of the system access control is to prevent unauthorised use of data processing systems used for the processing of Customer Data.

The following may, among other controls, be applied depending upon the particular Services ordered: authentication via complex passwords and/or multi-factor authentication, documented authorization processes, documented change management processes, and logging of access on several levels.

For all our services: (i) log-ins to data storage or processing systems are logged; (ii) logical access to the data storage and processing systems is restricted and protected by VLAN/VPN; and (iii) centralized logging and alerting, and firewalls are used.

Data Access Control
Technical and organisational measures regarding the authorisation concept, data access rights and monitoring and recording of the same:

Measures regarding data access control are targeted on the basis that only such data can be accessed for which an access authorisation exists and that data cannot be read, copied, changed or deleted in an unauthorised manner during the processing and after the saving of such data.

Customer Data is accessible and manageable only by properly authorized staff, direct database query access is restricted, and application access rights are established and enforced. Access to data necessary for the performance of the particular task is ensured within the systems and applications by a corresponding role and authorisation concept.

Transmission Control
Technical and organisational measures regarding the transport, transfer, transmission, storage and subsequent review of Customer Data on data media (manually or electronically).

Transmission control is implemented so that Customer Data cannot be read, copied, changed or deleted without authorisation, during transfer or while stored on data media, and so that it can be monitored and determined as to which particular recipients a transfer of Customer Data is intended.

Except as otherwise specified for the Service or parts thereof, transfers of data outside the Cloud Service environment are encrypted and/or stored on encrypted media.

The content of communications (including sender and recipient addresses) sent through some email or messaging services may not be encrypted. You as the customer are solely responsible for the results of your decision to use unencrypted communications or transmissions when exchanging data with us through such email or messaging services.

The transfer of Customer Data to a third party (e.g. sub-processors) is only made if a corresponding contract exists, and only for the specific purposes. If Customer Data is transferred to companies located outside the EEA, we provide that an adequate level of data protection exists at the target location or organisation in accordance with our obligations of this DPA, e.g. by employing contracts based on the Standard Contractual Clauses.

Customer Data used for internal purposes only e.g. as part of the respective customer relationship, may be transferred to a third party such as a subcontractor, solely under consideration of contractual arrangements and appropriate data protection regulatory requirements.

Data Processing Control
Technical and organisational measures regarding recording and monitoring of the circumstances of data processing to enable retroactive review:

For systems and/or electronic records in scope of Title 21, Part 11 of the Code of Federal Regulations, Data Processing Controls are implemented so that a retroactive review is enabled.

System inputs are recorded in the form of audit logs and electronic records therefore it is possible to review retroactively whether and by whom Customer Data was entered, altered or deleted.

Data Backup and Availability Control
Technical and organisational measures regarding data backup (physical/logical):

Data backup and availability controls are implemented to protect Customer Data against accidental destruction and loss.

Backups for our Hosting Infrastructure are taken on a regular basis and managed according to Julius Clinical's System Management Plan. The System Manage Plan also describes the agreed service levels and refers to our for Back-up and Recovery standard operating procedure which includes periodic reviews on backup, recovery and fail-over testing.

Backup media transferred outside of the Hosting infrastructure is always encrypted.

Bijlage 3: Afspraken betreffende Inbreuken in verband met Persoonsgegevens

Bij een Datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van Persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Onder een Datalek valt dus niet alleen het vrijkomen (lekken) van Persoonsgegevens, maar ook onrechtmatige verwerking van Persoonsgegevens.

De Opdrachtgever spreekt van een Datalek als er een inbreuk is op de beveiliging van persoonsgegevens. Bij een Datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking, dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden.

Informeren over Datalekken en/of incidenten met betrekking tot beveiliging
De Opdrachtgever dient als verwerkingsverantwoordelijke een Datalek te melden bij de Autoriteit Persoonsgegevens. Om aan deze plicht te kunnen voldoen dient de Opdrachtnemer zonder onredelijke vertraging rekenend vanaf het moment dat de Opdrachtnemer een Datalek heeft vastgesteld, dit te melden bij Functionele emailadres@rivm.nl en 5.1.2e @rivm.nl of per telefoon op 030 - 5.1.2e (telefoon alleen tijdens kantoortijden).

De Opdrachtnemer dient bij een melding expliciet aan te geven dat de melding een Datalek Persoonsgegevens betreft. De Opdrachtnemer ontvangt een datalek formulier die digitaal wordt aangeleverd bij datalekken.