

Concept VERWERKERSOVEREENKOMST

Kenmerk [...]

De ondergetekenden:

1. <<opdrachtgever informatie>>

hierna te noemen: **Opdrachtgever**

en

2. <<<Opdrachtnemer informatie>>>

te dezen rechtsgeldig vertegenwoordigd door:

hierna te noemen “**Verwerker**”,

De Opdrachtgever en Verwerker hierna afzonderlijk ook aan te duiden als “Partij” en gezamenlijk als “Partijen”;

overwogen als volgt:

- A. De Opdrachtgever heeft Verwerker opdracht gegeven Diensten te verrichten, zoals omschreven in de hoofdraamovereenkomst gesloten tussen Partijen op <DATUM>, getiteld [“TITEL”], <NUMMER>, hierna “**de Raamovereenkomst**”, waarbij Verwerker ten behoeve van de Opdrachtgever persoonsgegevens in de zin van de Algemene Verordening Gegevensbescherming (AVG) zal dienen te Verwerken;
- B. De Opdrachtgever en Verwerker wensen hun wederzijdse rechten en verplichtingen voor de Verwerking van Persoonsgegevens conform het vereiste van artikel 28 AVG vast te leggen in deze Verwerkersovereenkomst, en verklaren te zijn overeengekomen als volgt:

Artikel 1 Begrippen

In deze Verwerkersovereenkomst gelden de volgende definities:

- 1.1 **AP:**
De Autoriteit Persoonsgegevens.
- 1.2 **AVG:**
Verordening (EU) 2016/679 van het Europees parlement en de Raad van 27 april 2016 (de Algemene Verordening Gegevensbescherming).
- 1.3 **Betrokkene:**
Een geïdentificeerde of identificeerbare natuurlijk persoon op wie de Persoonsgegevens betrekking hebben.
- 1.4 **Bijlagen:**
De bijlagen bij deze Verwerkersovereenkomst, die integraal deel uitmaken van deze Verwerkersovereenkomst.
- 1.5 **Datalek (in de AVG aangeduid als ‘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 persoonsgegevens.
- 1.6 **Derde:**
Een natuurlijke of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de Opdrachtgever, noch de Verwerker, noch de personen die onder rechtstreeks gezag van de Opdrachtgever of Verwerker gemachtigd zijn om de Persoonsgegevens te Verwerken.
- 1.7 **Diensten:**
De door Verwerker uit hoofde van de Raamovereenkomst te leveren diensten zoals nader beschreven in de Raamovereenkomst.
- 1.8 **DPIA (Data Protection Impact Assessment)** of gegevensbeschermingseffectbeoordeling:
Instrument waarmee organisaties privacy risico's in een vroegtijdig stadium op een gestructureerde en heldere manier in kaart kunnen worden gebracht bij het bouwen van informatiesystemen of aanleggen van databestanden.
- 1.9 **Raamovereenkomst:**
De tussen de Opdrachtgever en Verwerker gesloten Raamovereenkomst zoals bedoeld in overweging A, inclusief de daarbij horende bijlagen, waaronder mede begrepen eventuele toepasselijke algemene voorwaarden van de Opdrachtgever dan wel Verwerker.
- 1.10 **Persoonsgegevens:**
Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de Betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identifier zoals een naam, een identificatienummer, locatiegegevens, een online identifier of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.
- 1.11 **Pseudonimisering:**
Het Verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.
- 1.12 **Privacywetgeving:**
Alle toepasselijke wet- en regelgeving met betrekking tot de Verwerking en bescherming van persoonsgegevens, waaronder maar niet beperkt tot de AVG, de Uitvoeringswet AVG en de e-Privacyrichtlijn zoals (in Nederland) geïmplementeerd in de Telecommunicatiewet, alsmede alle toekomstige, overeenkomstige of gerelateerde wetgeving al dan niet vastgesteld ter vervanging van voornoemde wetgeving.
- 1.13 **Subverwerker:**
Een partij die door Verwerker wordt ingeschakeld voor de uitvoering van de Raamovereenkomst en de daarbij horende Verwerking van Persoonsgegevens;
- 1.14 **Toestemming van de Betrokkene:**
Elke vrije, specifieke geïnformeerde en ondubbelzinnige wilsuiting waarmee de Betrokkene door middel van een verklaring of een ondubbelzinnige actieve handeling hem betreffende Verwerking van Persoonsgegevens aanvaardt.

- 1.15 **Toezichthouder:** een onafhankelijke instantie verantwoordelijk voor het toezicht op de naleving van wetgeving met betrekking tot de Verwerking van Persoonsgegevens, waaronder de AVG en de Uitvoeringswet. In Nederland is deze toezichthouder de Autoriteit Persoonsgegevens ("AP").
- 1.16 **Uitvoeringswet:**
Uitvoeringswet Algemene verordening gegevensbescherming.
- 1.17 **Verwerkersovereenkomst:**
De onderhavige verwerkersovereenkomst, inclusief de Bijlagen.
- 1.18 **Verwerking of het verwerken van persoonsgegevens:**
een bewerking of een geheel van bewerkingen 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, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Waar in deze Verwerkersovereenkomst termen worden gebruikt die niet in dit artikel 1 zijn gedefinieerd maar die wel in artikel 4 AVG gedefinieerd zijn, wordt aan deze termen de betekenis van de definities in artikel 4 AVG toegekend.

Artikel 2 Verwerking door Verwerker

- 2.1 De Opdrachtgever is ten aanzien van de in haar opdracht uit te voeren Verwerkingen van Persoonsgegevens de verantwoordelijke in de zin van artikel 4, zevende lid, AVG. Verwerker is verwerker in de zin van artikel 4, achtste lid, AVG.
- 2.2 Verwerker verwerkt de Persoonsgegevens slechts op basis van schriftelijke instructies van de Opdrachtgever, behoudens afwijkende wettelijke verplichtingen. Een overzicht van het onderwerp, de aard en de doeleinden van de Verwerking, het soort persoonsgegevens en de categorieën van betrokkenen, is uiteengezet in Bijlage I bij deze Verwerkersovereenkomst.
- 2.3 Verwerker verplicht zich om de van de Opdrachtgever verkregen Persoonsgegevens niet voor andere doeleinden of op andere wijze te gebruiken dan voor het doel/de doeleinden waarvoor de gegevens aan Verwerker zijn verstrekt of aan hem bekend zijn geworden. Het is Verwerker derhalve niet toegestaan andere gegevensverwerkingen uit te voeren dan door de Opdrachtgever (mondeling, schriftelijk dan wel elektronisch) aan Verwerker zijn opgedragen. Deze verplichting geldt zowel gedurende de looptijd van deze Verwerkersovereenkomst als na afloop daarvan.
- 2.4 Verwerker verplicht zich afdoende maatregelen te treffen om ervoor te zorgen dat iedere natuurlijke persoon die handelt onder het gezag van Verwerker en toegang heeft tot persoonsgegevens, deze slechts conform de bepalingen van deze Verwerkersovereenkomst verwerkt.
- 2.5 Verwerker heeft geen zeggenschap over het doel en de middelen voor de Verwerking van Persoonsgegevens en neemt geen zelfstandige beslissingen over het gebruik van de

Persoonsgegevens, de verstrekking aan Derden en de duur van de opslag van de Persoonsgegevens.

- 2.6 Verwerker verplicht zich te handelen conform de geldende Privacywetgeving.
- 2.7 Verwerker verschaft aan zijn medewerkers enkel toegang tot de Persoonsgegevens voor zover dit nodig is voor het verrichten van de Diensten op grond van de Raamovereenkomst.
- 2.8 Verwerker zal geen Persoonsgegevens aan een Derde verstrekken tenzij de verstrekking plaatsvindt in het kader van de uitvoering van deze Verwerkersovereenkomst, een uitdrukkelijke schriftelijke opdracht van de Opdrachtgever, op grond van een wettelijke verplichting of op bevel van een gerechtelijke of bestuurlijke instantie, en onder de voorwaarde dat Verwerker in het laatste geval de Opdrachtgever binnen 24 uur na ontvangst van een dergelijk bevel daarvan in kennis stelt om de Opdrachtgever in staat te stellen daartegen een eventueel haar ter beschikking staand rechtsmiddel in te stellen.
- 2.9 Indien Verwerker van oordeel is dat zij op grond van een wettelijke verplichting Persoonsgegevens ter beschikking dient te stellen aan een daartoe bevoegde instantie zal zij daar niet toe overgaan, dan na overleg met en goedkeuring van de Opdrachtgever. Zij zal de Opdrachtgever zo spoedig mogelijk schriftelijk in kennis stellen van de wettelijke verplichting en daarbij alle relevante informatie verstrekken die de Opdrachtgever redelijkerwijs nodig heeft om de benodigde maatregelen te treffen om te bepalen of verstrekking kan plaatsvinden en, zo ja, onder welke voorwaarden.
- 2.10 Verwerker geeft de Opdrachtgever op eerste verzoek inzage in het register van verwerkingsactiviteiten zoals bedoeld in artikel 30 lid 2 AVG met betrekking tot de Persoonsgegevens waarop deze Verwerkersovereenkomst betrekking heeft. Verwerker bedingt van ingeschakelde Subverwerkers dat de Opdrachtgever op eerste verzoek inzage krijgt in het register van verwerkingsactiviteiten als bedoeld in artikel 30 lid 2 AVG met betrekking tot de Persoonsgegevens waarop deze Verwerkersovereenkomst betrekking heeft.
- 2.11 Verwerker verbindt zich ertoe de Opdrachtgever bij te staan in de analyse van de vraag of een DPIA noodzakelijk is voor de Verwerking van de persoonsgegevens door Verwerker. Dit impliceert bijvoorbeeld dat indien de Verwerking door Verwerker het gebruik van nieuwe technologieën vereist, of indien de Verwerker het plausibel acht dat de gebruikte technologie als “nieuw” kan worden gekwalificeerd, Verwerker voor de start van de Verwerking van de persoonsgegevens de Opdrachtgever hiervan op de hoogte brengt.
- 2.12 Verwerker verbindt zich ertoe dat wanneer de Opdrachtgever een DPIA nodig acht, Verwerker de Opdrachtgever bij zal staan bij de uitvoering hiervan. Verwerker verstrekt de Opdrachtgever in zulk geval ten minste de hiernavolgende informatie:
 - 2.12.1 Een systematische beschrijving van de beoogde Verwerkingen;
 - 2.12.2 Een beoordeling van de noodzaak en evenredigheid van de Verwerkingen met betrekking tot de doeleinden opgenomen in de Raamovereenkomst;
 - 2.12.3 Een beoordeling van de risico's voor de rechten en vrijheden van de betrokkene(n);

- 2.12.4 De beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat voldaan is aan de AVG. Hierbij wordt rekening gehouden met de rechten en gerechtvaardigde belangen van de betrokkene(n) en andere personen in kwestie.
- 2.13 Verwerker start de Verwerking pas na de (evaluatie van de) DPIA en de schriftelijke instructies hiertoe van de Opdrachtgever.
- 2.14 Indien, naar haar mening, een verzoek of instructie van de Opdrachtgever een inbreuk oplevert op de AVG of andere toepasselijke Privacywetgeving, zal Verwerker de Opdrachtgever hiervan onmiddellijk in kennis stellen.
- 2.15 De kosten die Verwerker moet maken ter uitvoering van deze Verwerkersovereenkomst zijn of worden geacht te zijn begrepen in de opdrachtsom voor de Raamovereenkomst. Verwerker zal derhalve geen kosten bij de Opdrachtgever (kunnen) declareren die zien op de uitvoering van deze Verwerkersovereenkomst.

Artikel 3 Beveiligingsmaatregelen en controle

- 3.1. Rekening houdend 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, treft Verwerker met betrekking tot de Persoonsgegevens welke in opdracht van de Opdrachtgever worden verwerkt alle passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, die, waar passend, onder meer het volgende omvatten:
- 3.1.1. de Pseudonimisering en adequate versleuteling van Persoonsgegevens;
 - 3.1.2. het vermogen om op permanente basis de vertrouwelijkheid, integriteit en beschikbaarheid van de verwerkingssystemen en Diensten te garanderen;
 - 3.1.3. het vermogen om bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de Persoonsgegevens tijdig te herstellen;
 - 3.1.4. een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de Verwerking, waaronder mede begrepen maatregelen om zwakke plekken te identificeren ten aanzien van de Verwerking van Persoonsgegevens in de systemen die worden ingezet voor het verlenen van de Diensten aan de Opdrachtgever.
 - 3.1.5. maatregelen om te waarborgen dat enkel bevoegd personeel toegang heeft tot de Persoonsgegevens die in het kader van de Verwerkersovereenkomst worden verwerkt;
 - 3.1.6. het hanteren van een passend informatiebeveiligingsbeleid voor de Verwerking van de Persoonsgegevens;
 - 3.1.7. het verzekeren van de continuïteit van de Diensten en de portabiliteit van de Persoonsgegevens in geval van een beëindiging van de Raamovereenkomst.

- 3.2. Bij de beoordeling van het passende beveiligingsniveau wordt met name rekening gehouden met de verwerkingsrisico's, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.
- 3.3. De door Verwerker in acht te nemen beveiligingsmaatregelen worden nader beschreven in Bijlage II. Verwerker zal periodiek met een frequentie van eenmaal per jaar, de in Bijlage II beschreven maatregelen actualiseren.
- 3.4. Verwerker verstrekt ieder kalenderjaar dat deze Verwerkersovereenkomst voortduurt aan de Opdrachtgever een rapportage waarin verslag wordt gedaan van de Verwerking van de Persoonsgegevens. De rapportage bevat ten minste de volgende onderdelen:
- 3.4.1. een overzicht van beveiligingsincidenten datalekken en beveiligingsincidenten, ook indien die buiten het toepassingsbereik van de Verwerkersovereenkomst vallen, die zich in het verslagjaar binnen de organisatie van de Verwerker en/of diens Subverwerker(s) hebben voorgedaan;
- 3.4.2. een overzicht van de voorgenomen wijzigingen van beveiligingsmaatregelen.
- De Opdrachtgever is gerechtigd nadere voorwaarden en eisen te stellen waaraan de jaarlijkse rapportages moeten voldoen alsook de wijze waarop de rapportages worden ingediend.
- 3.5. De Opdrachtgever is te allen tijde gerechtigd de Verwerking van Persoonsgegevens, en in het bijzonder de door Verwerker in acht te nemen beveiligingsmaatregelen, te (doen) controleren. De controle wordt met inachtneming van een redelijke termijn aangekondigd. Verwerker is verplicht de Opdrachtgever of een in opdracht van de Opdrachtgever controlerende instantie toe te laten en alle in redelijkheid benodigde medewerking te verlenen, zodat de controle daadwerkelijk uitgevoerd kan worden. Verwerker draagt er tevens zorg voor dat de door hem ingeschakelde Subverwerkers hiertoe de redelijkerwijs benodigde medewerking zullen verlenen.
- 3.6. Verwerker verbindt zich om binnen een door de Opdrachtgever te bepalen redelijke termijn de Opdrachtgever, of de door de Opdrachtgever ingeschakelde derde, te voorzien van de verlangde informatie die benodigd is om een oordeel vormen over de naleving door Verwerker van deze Raamovereenkomst. De Opdrachtgever draagt ervoor zorg dat de door haar ingeschakelde derde verplicht is tot geheimhouding ten aanzien van alle informatie betreffende de controle, tenzij deze ter nakoming van enige wettelijke bepaling gehouden is informatie te verstrekken.
- 3.7. Verwerker staat er voor in de door of namens de Opdrachtgever aangegeven aanbevelingen, die strekken tot verbetering van de naleving van de bepalingen voortvloeiend uit de Privacywetgeving, binnen de daartoe door de Opdrachtgever in redelijkheid te bepalen termijn uit te voeren.
- 3.8. Partijen kunnen overeenkomen om ter controle van de door Verwerker getroffen beveiligingsmaatregelen gebruik te maken van een Third Party Memorandum (TPM) opgesteld door een onafhankelijke externe deskundige. Dit TPM komt dan – mits het voldoende inzicht geeft in de naleving door Verwerker van zijn verplichtingen uit hoofde van deze Verwerkersovereenkomst

- in de plaats van de door de Opdrachtgever of een door de Opdrachtgever ingeschakelde derde te verrichten audits.

- 3.9. Verwerker zal de door hem getroffen beveiligingsmaatregelen evalueren en verscherpen, aanvullen of verbeteren voor zover de eisen of (technologische) ontwikkelingen daartoe aanleiding geven.
- 3.10. Op eerste verzoek van de Opdrachtgever zal Verwerker alle of een gedeelte van de Persoonsgegevens in een door de Opdrachtgever gewenst, gangbaar formaat ter beschikking stellen aan de Opdrachtgever. Verwerker zal ervoor zorg dragen dat de Opdrachtgever te allen tijde toegang behoudt tot de Persoonsgegevens en zal in geval van een geschil tussen Partijen deze toegang niet blokkeren. Verwerker zal maatregelen treffen om ervoor te zorgen dat de Opdrachtgever ook in geval van faillissement of surséance van betaling van Verwerker of Subverwerkers toegang blijft houden tot de Persoonsgegevens.

Artikel 4 Datalekken

- 4.1. Indien Verwerker kennis heeft genomen van een Datalek, informeert Verwerker de Opdrachtgever onverwijld, doch uiterlijk binnen 24 uur na ontdekking. Verwerker hanteert hierbij de contactgegevens zoals weergegeven in Bijlage III van deze Verwerkersovereenkomst. Verwerker zal alle benodigde maatregelen nemen om (verdere) schending of inbreuken betreffende de Verwerking de Persoonsgegevens te voorkomen, of te beperken.
- 4.2. Verwerker stelt de Opdrachtgever in staat om passende vervolgstappen te nemen ten aanzien van een Datalek, waaronder het kunnen beoordelen van het Datalek en het tijdig en adequaat kunnen informeren van Toezichthouder(s) en Betrokkenen en verleent de Opdrachtgever alle daartoe redelijkerwijs benodigde medewerking. Verwerker zal in ieder geval informatie verstrekken ten aanzien van het volgende:
- (i) de aard van het Datalek, waar mogelijk onder vermelding van de categorieën van Betrokkenen in kwestie en (bij benadering) het aantal betrokkenen in kwestie;
 - (ii) de (mogelijk) getroffen Persoonsgegevens en (bij benadering), het aantal getroffen Persoonsgegevens in kwestie;
 - (iii) de vastgestelde en verwachte gevolgen van het Datalek voor de Verwerking van de Persoonsgegevens en de daarbij betrokken personen;
 - (iv) de maatregelen die Verwerker heeft getroffen en zal treffen om het Datalek aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele negatieve gevolgen van het Datalek.
- 4.3. In geval van een Datalek, zal de Opdrachtgever voldoen aan wettelijke meldingsplichten. Op verzoek van de Opdrachtgever zal Verwerker de Opdrachtgever hierin bijstaan en adviseren.
- 4.4. Verwerker zal niet zelfstandig, zonder medeweten en uitdrukkelijke schriftelijke toestemming van de Opdrachtgever, stappen ondernemen en/of enige communicatie doen uitgaan omtrent het Datalek.

Artikel 5 Procedure rechten betrokkenen

- 5.1. Een klacht, bezwaar of verzoek van een Betrokkene met betrekking tot de Verwerking van de Persoonsgegevens wordt door Verwerker onverwijld doorgestuurd naar de Opdrachtgever, die verantwoordelijk is voor de afhandeling van de klacht, het bezwaar of het verzoek.
- 5.2. Verwerker verleent de Opdrachtgever op eerste verzoek alle redelijke medewerking om de Opdrachtgever in staat te stellen binnen de wettelijke termijnen te voldoen aan de verplichtingen die uit hoofde van de Privacywetgevingen de Algemene wet of bestuursrecht of andere regelgeving op de Opdrachtgever rusten, waaronder doch niet uitsluitend verplichtingen met betrekking tot de uitoefening van de rechten van Betrokkenen zoals een verzoek om inzage, verbetering, aanvulling, verwijdering, afscherming, bezwaar maken tegen de Verwerking van - of een verzoek tot overdraagbaarheid van Persoonsgegevens.

Artikel 6 Aansprakelijkheid

- 6.1. Verwerker is aansprakelijk voor alle schade voortvloeiende uit of verband houdend met het door Verwerker en/of de door Verwerker ingeschakelde Subverwerker(s) niet-nakomen van de verplichtingen voortvloeiende uit deze Verwerkersovereenkomst dan wel enig ander handelen in strijd met de Privacywetgeving.
- 6.2. Verwerker vrijwaart de Opdrachtgever tegen aanspraken van derden, waaronder Betrokkenen, in verband met het tekortschieten van Verwerker en/of de door Verwerker ingeschakelde Subverwerker(s) in de nakoming van deze Verwerkersovereenkomst of enige overtreding door Verwerker en/of de door Verwerker ingeschakelde Subverwerker(s) van de Privacywetgeving en zal alle daarmee verband houdende en daaruit voortvloeiende kosten (waaronder mede begrepen de kosten van juridische bijstand) en schade van de Opdrachtgever (waaronder mede begrepen eventuele door een toezichthouder opgelegde boetes die aan Verwerker of diens Subverwerker(s) toerekenbaar zijn) vergoeden.

Artikel 7 Looptijd, rangorde, wijziging en beëindiging

- 7.1. De looptijd van deze Verwerkersovereenkomst is gelijk aan de looptijd van de tussen Partijen gesloten Raamovereenkomst, inclusief eventuele verlengingen daarvan.
- 7.2. Op deze Verwerkersovereenkomst zijn de Algemene voorwaarden dienstverlening van de Opdrachtgever voor overeenkomsten van opdracht tot het verrichten van diensten van toepassing, tenzij in de Raamovereenkomst anders is overeengekomen. Bij tegenstrijdigheid tussen bepalingen van deze Verwerkersovereenkomst enerzijds en de Raamovereenkomst en/of voornoemde Algemene Voorwaarden prevaleren de bepalingen van deze Verwerkersovereenkomst.
- 7.3. De Opdrachtgever en Verwerker treden met elkaar in overleg over wijzigingen in deze Verwerkersovereenkomst als een wijziging in regelgeving of een wijziging in de uitleg van

regelgeving, of een wijziging in de dienstverlening van de Opdrachtgever dan wel Verwerker daartoe aanleiding geven. Een wijziging van deze Verwerkersovereenkomst kan uitsluitend schriftelijk overeengekomen worden in een door beide partijen bevoegdlijk ondertekend document. Deze bevoegdheid kan niet worden uitgeoefend door een contactpersoon van de Opdrachtgever. Daar waar in deze Verwerkersovereenkomst de schriftelijkheidseis wordt gesteld wordt een e-mail daarmee gelijk gesteld, tenzij het een wijziging van deze Verwerkersovereenkomst betreft.

- 7.4. Deze Verwerkersovereenkomst eindigt van rechtswege bij de beëindiging van de Raamovereenkomst. De beëindiging van deze Verwerkersovereenkomst zal Partijen niet ontslaan van hun verplichtingen die voortvloeien uit deze Verwerkersovereenkomst die naar hun aard worden geacht ook na beëindiging voort te duren.
- 7.5. Iedere meer dan ondergeschikte tekortkoming ten aanzien van de verplichtingen uit hoofde van deze Verwerkersovereenkomst geldt als een zodanige (zware) tekortkoming dat de Opdrachtgever – onverminderd diens overige rechten - gerechtigd is om deze Verwerkersovereenkomst en de Raamovereenkomst per direct geheel of gedeeltelijk te ontbinden, zonder dat dit tot enige verplichting van de Opdrachtgever tot schadevergoeding leidt. Het optreden van een Datalek dat toerekenbaar is aan Verwerker en/of diens Subverwerker(s) geldt in ieder geval als een tekortkoming die een ontbinding rechtvaardigt. Onverlet diens rechten tot opzegging en/of ontbinding voortvloeiend uit de Raamovereenkomst is de Opdrachtgever, zonder dat dit tot enige verplichting van de Opdrachtgever tot schadevergoeding leidt, tevens gerechtigd deze Verwerkersovereenkomst en de Raamovereenkomst per direct te ontbinden indien Verwerker te kennen geeft of anderszins vast komt te staan dat zij niet (langer) kan voldoen aan zijn verplichtingen voortvloeiend uit deze Verwerkersovereenkomst of de betrouwbaarheidseisen die op grond van ontwikkelingen in de Privacywetgeving en/of de rechtspraak aan de Verwerking van persoonsgegevens worden gesteld.
- 7.6. Onverwijld na het eindigen van Verwerkersovereenkomst zal Verwerker op eerste verzoek alle Persoonsgegevens in een door de Opdrachtgever gewenst, gangbaar formaat ter beschikking stellen aan de Opdrachtgever.
- 7.7. Verwerker verplicht zich om de in opdracht van de Opdrachtgever verwerkte Persoonsgegevens bij de beëindiging van de Verwerkersovereenkomst en na verstrekking daarvan aan de Opdrachtgever op de door de Opdrachtgever aangegeven wijze te (doen) vernietigen, tenzij de Persoonsgegevens langer bewaard moeten worden, bijvoorbeeld in het kader van (wettelijke) verplichtingen, dan wel op schriftelijk verzoek van de Opdrachtgever.
- 7.8. Verwerker zal de Opdrachtgever schriftelijk of elektronisch bevestigen dat vernietiging van de Verwerkte persoonsgegevens heeft plaatsgevonden. De Opdrachtgever is gerechtigd een controle te laten uitvoeren of vernietiging heeft plaatsgevonden. Deze controle wordt uitgevoerd door een in overleg met Verwerker aan te wijzen onafhankelijke deskundige, die aan geheimhouding is gebonden. Verwerker zal aan een dergelijke controle zijn medewerking verlenen. De kosten voor de in te huren deskundige komen voor rekening van de Opdrachtgever, tenzij uit de controle blijkt dat Verwerker zich niet aan zijn verplichtingen uit hoofde van deze

Verwerkersovereenkomst heeft gehouden, in welk geval de kosten volledig voor rekening van Verwerker komen.

- 7.9. Verwerker zal de Subverwerker(s) die betrokken zijn bij de Verwerking van de Persoonsgegevens op de hoogte stellen van een beëindiging van de Verwerkersovereenkomst en zal waarborgen dat de Subverwerker(s) de Persoonsgegevens teruggeven en vervolgens op de door de Opdrachtgever aangegeven wijze (laten) vernietigen.

Artikel 8 Subverwerkers en plaats van Verwerking

- 8.1. Verwerker is slechts gerechtigd de uitvoering van de Diensten geheel of ten dele uit te besteden aan Subverwerkers na voorafgaande schriftelijke uitdrukkelijke toestemming van de Opdrachtgever. Subverwerkers waarvoor de Opdrachtgever bij aangaan van deze Verwerkersovereenkomst de hiervoor bedoelde toestemming heeft gegeven worden weergegeven in Bijlage I. Indien de Opdrachtgever toestemming heeft gegeven, draagt Verwerker ervoor zorg dat de betreffende Subverwerker bij schriftelijke Raamovereenkomst ten minste dezelfde verplichtingen inzake de Verwerking en bescherming van Persoonsgegevens oplegt als de verplichtingen die zijn opgenomen in deze Verwerkersovereenkomst, waaronder mede begrepen doch niet uitsluitend de verplichting afdoende garanties met betrekking tot het toepassen van passende technische en organisatorische maatregelen te bieden opdat de Verwerking aan het bepaalde in de toepasselijke Privacywetgeving voldoet.
- 8.2. De Opdrachtgever kan aan haar schriftelijke toestemming aanvullende voorwaarden verbinden, die door Verwerker aan de Subverwerker(s) moeten worden opgelegd.
- 8.3. Verwerker staat in voor de door hem ingeschakelde Subverwerker(s) en blijft in de verhouding tussen Partijen altijd aanspreekpunt en volledig verantwoordelijk en aansprakelijk voor de naleving van de bepalingen uit deze Raamovereenkomst, inclusief de naleving van de eventuele nadere voorwaarden als bedoeld in het voorgaande lid.
- 8.4. Verwerker verbindt zich toe te zien op de naleving van de in de artikelen 8.1 en 8.2 doorgezette plichten door de ingeschakelde Subverwerker(s).
- 8.5. Het is Verwerker behoudens voorafgaande schriftelijke toestemming van de Opdrachtgever niet toegestaan om Persoonsgegevens buiten de Europese Unie dan wel door een internationale organisatie te (doen) Verwerken, tenzij een op de Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling hem tot Verwerking verplicht in welk geval Verwerker de Opdrachtgever, voorafgaand aan de Verwerking, in kennis stelt van dat wettelijk voorschrift, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt. In alle gevallen garandeert Verwerker, onverminderd het bepaalde in dit artikel 8, dat zij en de eventueel door Verwerker met toestemming van de Opdrachtgever ingeschakelde Subverwerker(s) een passend niveau van bescherming van Persoonsgegevens waarborgen in de zin van de in Nederland geldende privacywetgeving en overlegt Verwerker daarvan voorafgaand aan de Verwerking buiten de Europese Unie schriftelijk bewijs aan de Opdrachtgever.

Artikel 9 Geheimhouding

- 9.1. Verwerker zorgt er voor dat een ieder, waaronder zijn werknemers, vertegenwoordigers en/of Subverwerker(s), die betrokken is bij de Verwerking van de Persoonsgegevens deze gegevens vertrouwelijk behandelt. Verwerker bewerkstelligt en staat ervoor in dat voor een ieder die betrokken is bij de Verwerking van de Persoonsgegevens een geheimhoudingsovereenkomst of –beding is gesloten.
- 9.2. De in dit artikel bedoelde geheimhoudingsplicht geldt niet voor zover de Opdrachtgever uitdrukkelijk schriftelijk toestemming heeft gegeven om de Persoonsgegevens aan een Derde te verstrekken, indien het verstrekken van de Persoonsgegevens aan een Derde noodzakelijk is gezien de aard van de door Verwerker aan de Opdrachtgever te verlenen Diensten, of indien er een wettelijke verplichting bestaat om de Persoonsgegevens aan een Derde te verstrekken. Het bepaalde in artikel 2.8 en 2.9 is hier mede van toepassing.

Artikel 10 Toepasselijk recht / Bevoegde rechter

- 10.1 Op deze Verwerkersovereenkomst is uitsluitend Nederlands recht van toepassing.
- 10.2 Alle geschillen die ontstaan naar aanleiding van deze Verwerkersovereenkomst worden beslecht op dezelfde wijze als opgenomen in de Raamovereenkomst.

- handtekeningenpagina volgt -

Ondertekening

Aldus overeengekomen en in tweevoud ondertekend:

Opdrachtgever

[naam Verwerker].

rechtsgeldig vertegenwoordigd door:

[naam]

[functie]

rechtsgeldig vertegenwoordigd door:

[naam]

[functie]

Datum: [dag-maand-jaar]

Datum: [dag-maand-jaar]

Bijlage I

Onderwerp, aard en doeleinden van de Verwerking

[Nader in te vullen. Beschrijf de dienstverlening van Verwerker en wat bereikt moet worden met de dienstverlening zo nauwkeurig mogelijk]

Categorieën persoonsgegevens

[Een omschrijving van de persoonsgegevens die verwerkt zullen worden. Bijvoorbeeld: naam, adres, telefoonnummer, e-mail]

Toelichting: Indien er gegevens van werknemers worden verwerkt in bijvoorbeeld personeels-/salarissysteem c.q. verzuimregistratiesysteem zullen dit er meer zijn. Denk bijvoorbeeld aan:

BSN, geboortedata, rekeningnummers, gegevens mbt arbeidsvoorwaarden, salarisgegevens, functie- en opleidingsgegevens, gegevens mbt functioneren, huisartsgegevens, verzuiminformatie, etc.

NB: gegevens die door de arbodienst worden verwerkt door of onder verantwoordelijkheid van een bedrijfsarts vallen niet onder de scope van een verwerkersovereenkomst. De arbo-dienst/bedrijfsarts is daarvoor zelf verantwoordelijk.

Categorieën van betrokkenen

[Een omschrijving van de (groepen) personen waarvan Persoonsgegevens Verwerkt worden, bijvoorbeeld burgers, (contactpersonen van) opdrachtnemers en overige relaties van de Opdrachtgever, en/of medewerkers van de Opdrachtgever]

Met toestemming van de Opdrachtgever ingeschakelde Subverwerkers [in te vullen door Verwerker indien van toepassing]

Verwerker heeft met toestemming van de Opdrachtgever de volgende Subverwerkers ingeschakeld die in opdracht van Verwerker (delen van) de Diensten (zullen) uitvoeren:

- i. <naam>B.V., gevestigd te <adres>, ten behoeve van de uitvoering van de volgende diensten:
[beschrijving werkzaamheden subverwerker];
- ii. <naam>B.V., gevestigd te <adres>, ten behoeve van de uitvoering van de volgende diensten:
[beschrijving werkzaamheden subverwerker];

Toelichting: Verwerker dient hier in te vullen van welke derden hij gebruik maakt bij het verwerken van de Persoonsgegevens ten behoeve van de Opdrachtgever. Denk ook aan eventuele hostingleveranciers waar de Verwerker de opslag en beheer van data aan heeft uitbesteed. Vóór het tekenen van deze Verwerkersovereenkomst dient de Opdrachtgever hiervan te beoordelen of zij hiervoor toestemming wil verlenen als bedoeld in artikel 8 van de Verwerkersovereenkomst.

Landen van Verwerking (in te vullen door Verwerker)

Verwerker verwerkt de Persoonsgegevens in de volgende landen:

[opsomming landen waar gegevens worden opgeslagen dan wel door Subverwerker(s) worden verwerkt]

Waarborgen in verband met Verwerking buiten de EER [in te vullen door Verwerker indien van toepassing]

[beschrijving van aanvullende maatregelen in verband met een eventuele verwerking van de Persoonsgegevens in landen buiten de EER.]

Toelichting: ook hier dient de Opdrachtgever na te gaan of een eventuele voorgenomen verwerking buiten de EER wel acceptabel is en of deze aan alle door de AVG daaraan gestelde eisen voldoet. De Verwerker dient hierover nadere informatie te verstrekken.

Denk hierbij ook aan cloudopslag! In dat verband kan al snel sprake zijn van doorgifte van gegevens naar landen buiten de EER (bijvoorbeeld servers van Microsoft Azure buiten de EER).

Indien sprake is van verwerking in landen buiten de EER dienen er aanvullende maatregelen te zijn getroffen, bijvoorbeeld het gebruik van door de Europese Commissie goedgekeurde modelcontracten voor doorgifte van gegevens of een Privacy Shield certificering.

Bijlage II

Overzicht beveiligingsmaatregelen, uitwerking van artikel 3 en 4 van de Verwerkersovereenkomst

Verwerker heeft een (informatie)beveiligingsbeleid opgesteld en de hierin beschreven maatregelen aantoonbaar geïmplementeerd. Dit beleid wordt met regelmaat getoetst en geactualiseerd. De beveiligingsmaatregelen zijn passend voor en in overeenstemming met de waarde van de te verwerken gegevens. Wanneer Verwerker gebruik maakt van Subverwerkers, dienen deze expliciet te zijn beschreven en bekend te zijn bij de Opdrachtgever. De Subverwerker houdt zich aan minimaal dezelfde beveiligingseisen en –maatregelen als Verwerker.

Organisatie van informatiebeveiliging

Verantwoordelijkheden ten aanzien van het beschermen van Persoonsgegevens zijn binnen de organisatie Verwerker expliciet benoemd en belegd.

Personele maatregelen

Verwerker heeft aantoonbaar bevoegd en bekwaam personeel. Zowel bevoegd en bekwaam voor het verwerken van de gegevens als voor het beveiligen en beschermen van de gegevens.

De personeelsleden zijn via een schriftelijke Raamovereenkomst verplicht tot geheimhouding van alle informatie van de Opdrachtgever.

Toegang tot Persoonsgegevens

Toegang tot Persoonsgegevens is beperkt op basis van het need-to-know principe. Alleen wanneer toegang tot Persoonsgegevens daadwerkelijk benodigd is voor het uitvoeren van de werkzaamheden wordt deze toegang ook ingeregeld. Zodra bevoegdheden van personen veranderen, wordt de toegang tot gegevens hierop aangepast.

Verwerking op mobiele apparatuur

Wanneer Persoonsgegevens worden verwerkt op mobiele apparatuur, waaronder tablets, laptops en/of smartphones, dan dienen deze apparaten versleuteld (encrypted) te zijn conform marktstandaarden.

Fysieke beveiliging

Verwerker zorgt ervoor dat Persoonsgegevens worden verwerkt in een fysiek beveiligde omgeving, met passende bescherming tegen dreigingen van buitenaf.

IT-technische maatregelen

Verwerker neemt passende maatregelen om de IT-omgeving te beveiligen. Informatiesystemen, componenten en middelen zijn actueel en worden door de fabrikant officieel ondersteund.

Alle software wordt op basis van een gestructureerd proces voorzien van de laatste patches. Waar technisch mogelijk wordt gebruik gemaakt van antivirussoftware.

Netwerken en informatiesystemen worden passend afgeschermd op basis van fysieke of logische scheiding, waarbij wordt gewaarborgd dat informatie van de Opdrachtgever niet vermengd kan worden met dat van andere klanten van Verwerker.

Wanneer informatie over openbare netwerken of anderszins publiek beschikbaar kan komen, worden cryptografische maatregelen genomen om de informatie te beschermen tegen onbevoegde inzage.

Periodiek, doch ten minste eenmaal per jaar, worden vulnerability scans en penetratietests uitgevoerd voor het toetsen van de beveiliging.

Toegang op afstand

Wanneer medewerkers van Verwerker toegang op afstand (bijvoorbeeld telewerken via internet)

kunnen krijgen tot Persoonsgegevens, is deze toegang afgeschermd met een versleutelde verbinding. Toegang op afstand kan alleen worden verkregen door middel van het toepassen van 2 factor authenticatie.

Beheer van incidenten

Verwerker verplicht zijn medewerkers incidenten met betrekking tot informatiebeveiliging en privacy zo snel mogelijk te melden en deze op basis van de ernst op te volgen. Enkele voorbeelden van incidenten zijn:

- Uitval van dienstverlening, apparatuur of voorzieningen;
- Systeemstoringen of –overbelasting;
- Niet-naleven van beleid en/of richtlijnen;
- Inbreuk op fysieke beveiligingsmaatregelen;
- Ongecontroleerde systeemwijzigingen;
- Storingen aan software of hardware;
- Verlies van gegevens of onbevoegde toegang tot gegevens;
- Malwarebesmetting;
- Toegangsovertredingen (digitaal of fysiek).

Alle medewerkers, tijdelijke medewerkers, onderaannemers en derde partijen die op enigerlei wijze gebruik maken van informatie of informatiesystemen van Verwerker zijn verplicht om (mogelijke) lekken en inbreuken in de informatiebeveiliging te melden als incident. Hiertoe wordt aan deze betrokkenen het incidentmeldingsproces van Verwerker kenbaar gemaakt.

Verwerker monitort toegang tot Persoonsgegevens en het mogelijk lekken hiervan.

Continuïteit van de dienstverlening

Verwerker neemt binnen de dienstverlening passende technische en organisatorische maatregelen om continuïteit te waarborgen. Wanneer de Raamovereenkomst tussen de Opdrachtgever en Verwerker eindigt, verplicht Verwerker zich te zorgen dat de dienstverlening van de Opdrachtgever gewaarborgd blijft in de transitie naar de nieuwe opdrachtnemer van de Opdrachtgever.

Overige maatregelen

De maatregelen beschreven in deze bijlage pretenderen niet concreet of volledig te zijn. De Opdrachtgever verwacht dat Verwerker zich actief opstelt bij het beschermen van Persoonsgegevens en het nemen van maatregelen om deze te beschermen. In wederzijds overleg kunnen verbeteringen ten aanzien van de Verwerkersovereenkomst en de beschreven maatregelen worden besproken.

Bijlage III

Contactpersonen Opdrachtgever en Verwerker (opdrachtnemer van Opdrachtgever) inzake melding Datalek

In geval van melding van een Datalek dient Verwerker onverwijld contact op te nemen met de hieronder weergegeven contactpersoon of bij diens afwezigheid met servicedesk van Opdrachtgever

Contactpersoon Opdrachtgever:	[naam, mobiele tel. nr., e-mailadres]
Vervanger 1:	[naam, mobiele tel. nr., e-mailadres]
Vervanger 2:	[naam, mobiele tel. nr., e-mailadres]

Contactpersoon Verwerker:	[naam, mobiele tel. nr., e-mailadres]
Vervanger 1:	[naam, mobiele tel. nr., e-mailadres]
Vervanger 2:	[naam, mobiele tel. nr., e-mailadres]