OVEREENKOMST VOOR GEGEVENSVERWERKING

tussen

Klant / Firma
Verantwoordelijke
Adres

- hierna genoemd: Opdrachtgever

en

Idiligo B.V.
Kabelweg 57
NL-1014 Amsterdam

- hierna genoemd: Verwerker

wordt de volgende overeenkomst gesloten:

§ 1 Preambule

De contractpartijen bereiden zich voor op of hebben reeds een zakelijke relatie. Deze overeenkomst specificeert de verplichtingen van de contractpartijen op vlak van gegevensbescherming, die voortvloeien uit de onderliggende overeenkomst (hierna: 'hoofdovereenkomst') waarin de gegevensverwerking in detail is beschreven. De activiteit die in de bovengenoemde overeenkomst wordt beschreven, is de verwerking van gegevens. Het is daarom noodzakelijk dat de contractpartijen een overeenkomst sluiten over de verwerking van gegevens volgens art. 28 van de Europese Algemene Verordening Gegevensbescherming (AVG).
Deze overeenkomst is van toepassing op alle activiteiten die verband houden met de hoofdovereenkomst en waarbij medewerkers van de verwerker of personen die in opdracht van de verwerker persoonlijke gegevens van de opdrachtgever verwerken.

§ 2 Verantwoordelijkheid

(1) In het kader van deze overeenkomst is de opdrachtgever verantwoordelijk voor de naleving van de wettelijke bepalingen, met name de rechtmatigheid van de gegevensverwerking ('verantwoordelijke' in de zin van art. 4, nr. 7 AVG).
(2) De verwerker houdt zelf een lijst bij van de door hem uitgevoerde verwerkingsactiviteiten in de zin van art. 30 AVG. Op verzoek verstrekt hij de opdrachtgever de informatie die nodig is voor het overzicht overeenkomstig art. 30 AVG.
(3) Indien de verwerker, in strijd met deze overeenkomst en de AVG, zelf de doeleinden en middelen van de verwerking bepaalt, wordt de verwerker beschouwd als de verantwoordelijke voor deze verwerking in de zin van art. 4, nr. 7 AVG.

§ 3 Definities

(1) ‘Verwerker’ is een natuurlijke persoon of rechtspersoon, overheidsinstantie, instelling of andere instantie die persoonlijke gegevens verwerkt in opdracht van de verantwoordelijke;
(2) ‘Persoonlijke gegevens’ zijn alle gegevens die betrekking hebben op een geïdentificeerde of identificeerbare natuurlijke persoon (hierna ‘betrokkene’ genoemd);
(3) ‘Verwerking’ is elk proces of elk geheel van processen dat al dan niet met behulp van geautomatiseerde processen wordt uitgevoerd met betrekking tot persoonlijke gegevens, zoals het verzamelen, registreren, organiseren, ordenen, bewaren, aanpassen of wijzigen, uitlezen, opvragen, gebruiken, openbaar maken door verzending, verspreiding of enige andere vorm van ter beschikking stelling, vergelijken of koppelen, beperken, verwijderen of vernietigen;
(4) ‘Instructie’ is elke instructie van de opdrachtgever gericht op een bepaalde gegevensbeschermende omgang (bijvoorbeeld anonimisering, blokkering, wissing, teruggave) van de orderverwerker met persoonlijke gegevens.
(5) ‘Onderaannemer’ is elke andere verwerker van de verwerker in de zin van art. 28, lid 4 AVG.
(6) ‘Derde’ is elke natuurlijke persoon of rechtspersoon, overheidsinstantie, instelling of andere instantie, met uitzondering van de betrokkene, de verantwoordelijke, de verwerker en de personen die onder het rechtstreekse gezag van de verantwoordelijke of de verwerker bevoegd zijn om de persoonlijke gegevens te verwerken;
(7) ‘Derde land’ is elk land buiten de Europese Unie en de Europese Economische Ruimte.

§ 4 Onderwerp en duur van de opdracht/de verwerking

(1) Het onderwerp van de opdracht vloeit voort uit de hoofdovereenkomst, waarnaar hier wordt verwezen.
(2) Voor zover het onderwerp niet of niet volledig uit de hoofdovereenkomst voortvloeit, is het onderwerp van de verwerking: Idiligo B.V. verleent de opdrachtgever een niet-overdraagbare, niet-exclusieve licentie voor het gebruik van de Idiligo-applicatie, in overeenstemming met de bepalingen van de ‘Algemene Voorwaarden, 3. Licentie en gebruik’ van Idiligo B.V., in detail:
    a) Idiligo geeft toegang tot de Idiligo-applicatie (gebruikerslogin via de website van Idiligo B.V.)
    b) Met de Idiligo-applicatie kan de opdrachtgever eigen gebruikers voor zijn Idiligo-account aanmaken
    c) De opdrachtgever kan zelf scripts ontwikkelen en gebruiken. Met deze scripts kan hij bijvoorbeeld ook klantspecifieke informatie documenteren.
    d) De opdrachtgever krijgt toegang tot zijn gedocumenteerde informatie.
(3) De duur van de opdracht is afhankelijke van de duur van de hoofdovereenkomst, tenzij anders vermeld in de bepalingen van deze overeenkomst.
(4) Het recht op onmiddellijke opzegging om zwaarwegende redenen blijft onaangetast.

§ 5 Omvang, type en doel van de verwerking, evenals soorten van persoonlijke gegevens en categorieën van betrokkenen

(1) Indien de omvang, het type en het doel van de verwerking nog niet in de hoofdovereenkomst zijn gespecificeerd, zijn de volgende bepalingen aanvullend van toepassing.

(2) Met name de volgende gegevens maken deel uit van de gegevensverwerking

Soorten van gegevens	**Categorieën van betrokkenen van de opdrachtgever**
Persoonlijke stamgegevens	Klanten
Contactgegevens (e-mail, telefoon)	Medewerkers
Klantgegevens	Geïnteresseerde personen
Communicatiegegevens (audio- en videostreaming, screensharing)	Sollicitanten
Inhoudelijke gegevens (gedeelde bestanden in scripts, tekstchat, whiteboard-inhoud)	Leveranciers
Activiteitenlogboeken (logbestanden)	Abonnees
Handtekeninggegevens (karaktereigenschappen van de digitale handtekening)	Opdrachtnemers
Contractgegevens (onderliggende juridische documenten met digitale handtekening)	Verkoopvertegenwoordigers / Partners
Kalendergegevens (datum, duur)	Zelfstandige medewerkers
	Gesprekspartner van de opdrachtgever
Supportticketgegevens (berichten en chatgesprekken tussen gebruikers en de opdrachtnemer in het kader van support-aanvragen)	
Metadata (gebruiksstatistieken) • Activiteitenlogboeken (logbestanden) • IP-adressen • Cookies • API traffic • Control/Signalisatie traffic • Mediaserver logbestanden • Platformtoegang logbestanden	

§ 6 Bevoegdheid om instructies te geven

(1) De verwerking van persoonlijke gegevens door de verwerker vindt uitsluitend plaats in het kader van de gemaakte afspraken en volgens de gedocumenteerde instructies van de opdrachtgever, tenzij er sprake is van een uitzonderlijk geval in de zin van art. 28, lid 3a AVG. Voor zover de opdrachtgever het nodig acht, kunnen personen worden benoemd die bevoegd zijn om instructies te geven. De opdrachtgever zal de verwerker hiervan schriftelijk of in tekstvorm op de hoogte brengen. Indien deze personen die bevoegd zijn om instructies te geven, veranderen bij de opdrachtgever, wordt de verwerker hiervan schriftelijk of in tekstvorm op de hoogte gebracht onder vermelding van de nieuwe persoon (personen).

(2) De instructies worden in eerste instantie in de hoofdovereenkomst vastgelegd en kunnen door de opdrachtgever vervolgens aan de door de verwerker aangewezen instantie schriftelijk of in elektronische vorm (tekstvorm) worden gewijzigd, aangevuld of vervangen (individuele instructies). Instructies die niet in de hoofdovereenkomst zijn opgenomen, zullen worden behandeld als een verzoek tot verandering van de uitvoering.

(3) Mondelinge instructies moeten onmiddellijk schriftelijk of in tekstvorm worden bevestigd.

(4) De verwerker brengt de opdrachtgever meteen op de hoogte indien hij van mening is dat een instructie in strijd is met de geldende wetgeving. De verwerker mag de uitvoering van de instructie opschorten totdat deze door de opdrachtgever is bevestigd of gewijzigd.

(5) De verwerker garandeert dat hij zijn medewerkers die betrokken zijn bij de gegevensverwerking van de opdrachtgever en andere personen die voor hem werken verbiedt om de gegevens buiten het kader van de instructies te verwerken.

(6) Veranderingen aan het onderwerp van de verwerking en proceswijzigingen vallen onder de instructiebevoegdheid van de opdrachtgever en moeten dienovereenkomstig worden gedocumenteerd. In het geval van een wijziging die de verwerker als substantieel beschouwt, heeft de verwerker het recht om bezwaar te maken. Indien de opdrachtgever ondanks het bezwaar van de verwerker op de wijziging aandringt, moet deze wijziging als een zwaarwegende reden worden beschouwd en maakt deze een onmiddellijke beëindiging van de OV-overeenkomst mogelijk waarop de instructie betrekking heeft, evenals de componenten van de betreffende hoofdovereenkomst waarop de OV-overeenkomst betrekking heeft.

Veranderingen aan het onderwerp van de verwerking en proceswijzigingen vallen onder de instructiebevoegdheid van de opdrachtgever en moeten dienovereenkomstig worden gedocumenteerd. Bij een substantiële wijziging van de opdracht heeft de verwerker het recht om bezwaar te maken. Indien de opdrachtgever ondanks het bezwaar van de verwerker op de wijziging aandringt, moet deze wijziging als een zwaarwegende reden worden beschouwd en maakt deze een onmiddellijke beëindiging van de OV-overeenkomst mogelijk waarop de instructie betrekking heeft, evenals de componenten van de betreffende hoofdovereenkomst waarop de OV-overeenkomst betrekking heeft.

§ 7 Plaats van uitvoering / overdracht naar een derde land

De verwerker zal de contractuele diensten in de Europese Unie (EU) of in de Europese Economische Ruimte (EER) of in een derde land leveren. Eventuele onderaannemers zullen de betreffende diensten in de Europese Unie (EU) of in de Europese Economische Ruimte (EER) of in een derde land leveren. Indien de verwerker of een onderaannemer diensten in een derde land levert, waarborgt de verwerker de naleving van de betreffende bepalingen van de AVG en levert hij daarvan het bewijs op verzoek van de opdrachtgever.

(1) Voor zover de gegevensverwerking in overeenstemming met deze overeenkomst en de wettelijke bepalingen voor de verwerking van persoonlijke gegevens voor de opdrachtgever of voor de overdracht van persoonlijke gegevens naar het buitenland buiten Duitsland mag worden uitgevoerd, is de verwerker verantwoordelijk voor de naleving en uitvoering van de wettelijke vereisten om een adequaat niveau van gegevensbescherming te garanderen in geval van verhuizing en grensoverschrijdend dataverkeer.

§ 8 Bescherming van gegevensgeheimen/vertrouwelijkheid en bedrijfsgeheimen

(1) De verwerker zorgt ervoor dat de personen die voor het verwerken van de persoonlijke gegevens bevoegd zijn, zich ertoe verbonden hebben de vertrouwelijkheid te bewaren of dat zij onderworpen zijn aan een passende wettelijke geheimhoudingsplicht. De verplichting tot vertrouwelijkheid en geheimhouding blijft bestaan, ook nadat de opdracht is beëindigd.

(2) Bovendien is de verwerker verplicht om alle kennis van bedrijfsgeheimen en gegevensbeveiligingsmaatregelen van de opdrachtgever die hij in het kader van de contractuele relatie heeft verkregen, vertrouwelijk te behandelen.

(3) Bovendien zijn alle personen van de verwerker verplicht om de bedrijfsgeheimen van de opdrachtgever te bewaren en moeten zij op de hoogte worden gebracht van §4 GeschGehG.

§ 9 Technische en organisatorische maatregelen

(1) In het kader van zijn verantwoordelijkheid zal de verwerker zijn interne organisatie zo inrichten dat deze voldoet aan de bijzondere eisen van de gegevensbescherming. Om de persoonlijke gegevens van de opdrachtgever adequaat te beschermen, zal hij technische en organisatorische maatregelen nemen die voldoen aan de vereisten van de AVG (art. 28, lid 3, punt c, 32 AVG).

(2) De verwerker dient dergelijke technische en organisatorische maatregelen te nemen zodat de vertrouwelijkheid, integriteit, beschikbaarheid en draagkracht van de systemen en diensten in verband met de verwerking op lange termijn gewaarborgd is.

(3) De verwerker garandeert dat hij zijn verplichtingen nakomt volgens art. 32, lid 1, punt d) AVG door een procedure te gebruiken waarbij regelmatig de doeltreffendheid van de technische en organisatorische maatregelen wordt gecontroleerd om de veiligheid van de verwerking te waarborgen.

(4) Voor de naleving van de overeengekomen beveiligingsmaatregelen geldt zoals overeengekomen het volgende

- Voor naleving van de overeengekomen beveiligingsmaatregelen en hun beproefde effectiviteit wordt verwezen naar de goedgekeurde gedragsregels overeenkomstig art. 40 AVG, waaraan de verwerker zich op 25 september 2020 heeft onderworpen en waarvan de naleving op 6 oktober 2020 is gecontroleerd en bevestigd.

(5) De verwerker behoudt zich het recht voor om de genomen beveiligingsmaatregelen te wijzigen, maar er moet steeds voor worden gezorgd dat het contractueel overeengekomen beschermingsniveau niet wordt onderschreden.

(6) De verwerker moet voor het begin van de verwerking de uitvoering van de vereiste technische en organisatorische maatregelen die voorafgaand aan de gunning van de overeenkomst zijn beschreven, in het bijzonder met betrekking tot de specifieke uitvoering van de overeenkomst, documenteren en deze ter beoordeling en goedkeuring aan de opdrachtgever overhandigen.

(7) Een beschrijving van de overeengekomen technische en organisatorische maatregelen is opgenomen in bijlage 1 bij deze overeenkomst.

§ 10 Relaties met onderaannemers, verdere verwerkers (onderaannemers)

(1) Onderaannemingsrelaties in de zin van deze verordening zijn diensten die rechtstreeks verband houden met de levering van de dienst uit de hoofdovereenkomst. Hieronder vallen niet de ondersteunende diensten die de verwerker gebruikt, zoals telecommunicatiediensten, post- en transportdiensten, onderhoud en gebruikersdiensten of de verwijdering van datadragers, evenals andere maatregelen om de vertrouwelijkheid, beschikbaarheid, integriteit en draagkracht van de hardware en software van gegevensverwerkingssystemen te waarborgen.
Om de bescherming en de beveiliging van de gegevens van de opdrachtgever te garanderen, is de verwerker echter verplicht om geschikte en wettelijk conforme contractuele overeenkomsten te sluiten en controlemaatregelen te nemen om de gegevens van de opdrachtgever te beschermen, ook in het geval van uitbestede ondersteunende diensten.

(2) De opdrachtgever geeft de verwerker de volmacht om verdere verwerkers (onderaannemers) in te schakelen in overeenstemming met de paragrafen in § 10 van deze overeenkomst. Deze machtiging vormt een algemene schriftelijke goedkeuring in de zin van art. 28, lid 2 AVG.

(3) De overdracht van de persoonlijke gegevens van de verwerker aan de onderaannemer en zijn eerste handeling is pas toegestaan nadat aan alle voorwaarden voor onderaanneming is voldaan.

(4) Indien de onderaannemer de overeengekomen dienst buiten de EU/EER levert, zorgt de verwerker voor de toelaatbaarheid volgens de wet inzake gegevensbescherming door passende maatregelen te nemen. Hetzelfde geldt wanneer dienstverleners in de zin van lid 1, zin 2 worden ingezet.

(5) Voor elke verdere uitbesteding door de onderaannemer is de uitdrukkelijke toestemming van de hoofdopdrachtgever nodig (ten minste in tekstvorm), alle contractuele bepalingen in de contractuele keten moeten ook aan de verdere onderaannemer worden opgelegd.

(6) Op het moment van het sluiten van deze overeenkomst treden de in bijlage 3 genoemde bedrijven op als onderaannemers voor deelprestaties voor de verwerker en verwerken en/of gebruiken zij in dit kader ook rechtstreeks de gegevens van de opdrachtgever. Voor deze onderaannemers wordt de toestemming tot handelen geacht te zijn gegeven.

(7) De opdrachtgever kan alleen om zwaarwegende redenen bezwaar maken tegen de inschakeling van een onderaannemer.

§ 11 Correctie, wissing en blokkering van gegevens

(1) Tijdens de lopende opdracht corrigeert, wist of blokkeert de verwerker de contractuele gegevens alleen in overeenstemming met de instructies van de opdrachtgever.

(2) Als een betrokkene rechtstreeks contact opneemt met de verwerker om zijn gegevens te corrigeren, te wissen of te blokkeren, zal de verwerker dit verzoek onmiddellijk naar de opdrachtgever doorsturen.

§ 12 Ondersteuning door de verwerker bij verplichtingen op grond van art. 12 - 23, 33-36 AVG

(1) De verwerker ondersteunt de opdrachtgever in het kader van zijn mogelijkheden bij het voldoen aan de vragen en aanspraken van de betrokken personen conform conform art. 12-23 AVG (informatieplicht, rechten van betrokkenen, recht op vergetelheid, recht op dataportabiliteit, enz.)

(2) De verwerker ondersteunt de opdrachtgever bij het vervullen van de informatieplicht ten aanzien van de respectieve toezichthoudende autoriteit of de personen die betrokken zijn bij een inbreuk op de bescherming van persoonlijke gegevens volgens art. 33, 34 AVG.

(3) De verwerker ondersteunt de opdrachtgever bij de beoordeling van de gevolgen voor de gegevensbescherming volgens art. 35 AVG met alle informatie waarover hij beschikt. Indien een voorafgaand overleg met de bevoegde toezichthoudende autoriteit nodig is conform art. 36 AVG, zal de verwerker de opdrachtgever ook hierin ondersteunen.

§ 13 Meldingsplichten van de verwerker

(1) De verwerker brengt de opdrachtgever onmiddellijk op de hoogte

a) in geval van inbreuken door de verwerker of de personen die bij hem in dienst zijn in het kader van de overeenkomst, tegen de bepalingen inzake de bescherming van persoonlijke gegevens van de opdrachtgever of tegen de in de overeenkomst opgenomen bepalingen. Hij neemt de nodige maatregelen om de gegevens te beveiligen en eventuele negatieve gevolgen voor betrokkenen te beperken en bespreekt dit rechtstreeks met de opdrachtgever;

b) als hij van mening is dat een instructie in strijd is met de geldende wetgeving;
c) over controlemaatregelen en maatregelen van de toezichthoudende autoriteiten, voor zover deze betrekking hebben op het onderwerp van deze overeenkomst. Dit geldt ook wanneer een bevoegde autoriteit in het kader van een administratieve of strafrechtelijke procedure een onderzoek instelt naar de verwerking van persoonlijke gegevens in verband met de gegevensverwerking bij de verwerker.

(2) Indien de gegevens van de opdrachtgever bij de bewerker in gevaar komen door inbeslagname of confiscatie, een insolventie- of faillissementsprocedure of andere gebeurtenissen of maatregelen van derden, zal de verwerker de opdrachtgever hiervan onmiddellijk op de hoogte brengen. De verwerker zal in deze context alle verantwoordelijken onmiddellijk informeren dat de soevereiniteit en de eigendom van de gegevens uitsluitend bij de opdrachtgever als 'verantwoordelijke' in de zin van de Algemene Verordening Gegevensbescherming berust.

§ 14 Teruggave en wissing van gegevens en datadragers bij einde overeenkomst

(1) Na afloop van de verwerkingsdiensten moet de verwerker alle persoonlijke gegevens naar keuze van de opdrachtgever verwijderen of teruggeven, tenzij er op grond van het recht van de Unie of het nationale recht dat op de verwerker van toepassing is, een verplichting bestaat om de persoonlijke gegevens op te slaan. Het logboek van de wissing moet op verzoek worden verstrekt

(2) Indien vervoer van het opslagmedium voor wissing noodzakelijk is, zal de verwerker geschikte maatregelen nemen om het te beveiligen, in het bijzonder tegen diefstal, ongeoorloofd lezen, kopiëren of wijzigen. De maatregelen en de toe te passen verwijderingsprocedure worden, naast de dienstbeschrijvingen, zo nodig in detail overeengekomen.

(3) Documentatie die dient als bewijs van de correcte en ordelijke gegevensverwerking, moet door de verwerker na afloop van de overeenkomst met inachtneming van de respectieve bewaartermijnen worden opgeslagen. Voor zijn ontlasting kan hij ze na afloop van de overeenkomst aan de opdrachtgever verstrekken.

(4) Indien de opdrachtgever niet in staat is om de gegevens terug te nemen, zal hij de verwerker hiervan tijdig schriftelijk op de hoogte brengen. De verwerker heeft dan het recht om namens de opdrachtgever persoonlijke gegevens te verwijderen.

(5) In het geval van afgekeurd en testmateriaal is een individuele opdracht tot verwijdering niet vereist; deze moeten worden verwijderd.

§ 15 Controlerechten van de opdrachtgever en gedoog- en participatierechten

(1) De verwerker levert de opdrachtgever met geschikte middelen het bewijs dat hij de in deze overeenkomst vastgelegde verplichtingen nakomt.

(2) De verwerker kan met name bewijs leveren door de volgende informatie te verstrekken:
    a) uitvoering van een interne audit
    b) attest van een expert
    c) interne bedrijfsgedragsregels inclusief extern bewijs van de naleving ervan
    d) certificaat voor gegevensbescherming en/of informatiebeveiliging (bijv. ISO 27001)
    e) goedgekeurde gedragsregels volgens art.40 AVG
    f) certificaten volgens art. 42 AVG

(3) Indien de door de opdrachtgever ingeschakelde auditeur een concurrentieverhouding met de verwerker heeft, heeft de verwerker het recht om hiertegen bezwaar te maken.
(4) De uitvoering van de opdrachtcontrole door middel van regelmatige controles door de opdrachtgever met betrekking tot de uitvoering of nakoming van de overeenkomst, met name de naleving en, indien nodig, de noodzakelijke aanpassing van voorschriften en maatregelen voor de uitvoering van de opdracht wordt door de verwerker ondersteund. De verwerker verbindt zich er in het bijzonder toe om op schriftelijk verzoek, eventueel ook in elektronisch formaat, binnen een redelijke termijn alle informatie te verstrekken die nodig is voor het uitvoeren van een controle.
(5) De opdrachtgever zal de verwerker onmiddellijk en volledig informeren indien hij tijdens de controle fouten of onregelmatigheden met betrekking tot de wet inzake gegevensbescherming ontdekt.

§ 16 Aanstelling van een functionaris voor gegevensbescherming

(1) De verwerker stelt een functionaris voor gegevensbescherming aan, voor zover aan de vereisten van art. 37 AVG wordt voldaan.
(2) Een wijziging van de functionaris voor gegevensbescherming moet onmiddellijk schriftelijk of in tekstvorm aan de opdrachtgever worden meegedeeld. De verwerker zorgt ervoor dat aan de vereisten voor de functionaris voor gegevensbescherming en zijn activiteiten overeenkomstig art. 38 AVG wordt voldaan.
(3) Indien er bij de verwerker geen functionaris voor gegevensbescherming is aangesteld, zal de verwerker een contactpersoon voor de opdrachtgever aanwijzen.
(4) Als de vestigingsplaats van de verwerker zich buiten de Unie bevindt, wijst hij een vertegenwoordiger in de Unie aan conform art. 27, lid 1, 3, lid 2 AVG.
(5) De personen die volgens lid 1-4 moeten worden aangesteld, worden vermeld in bijlage 2 bij deze overeenkomst.

§ 17 Aansprakelijkheid

(1) Opdrachtgever en verwerker zijn gezamenlijk aansprakelijk jegens de betreffende betrokkene voor schade die wordt veroorzaakt door een verwerking die niet in overeenstemming is met de AVG.

(2) De verwerker is uitsluitend aansprakelijk voor schade die het gevolg is van door hem uitgevoerde verwerkingen waarbij
    a) hij niet heeft voldaan aan de verplichtingen die voortvloeien uit de AVG en specifiek zijn opgelegd aan verwerkers, of
    b) hij in strijd met de rechtmatig gegeven instructies van de opdrachtgever heeft gehandeld of
    c) hij tegen de rechtmatig gegeven instructies van de opdrachtgever in heeft gehandeld.

(3) Voor zover de opdrachtgever verplicht is tot het betalen van een schadevergoeding aan een betrokkene, behoudt hij zich het recht voor om een beroep te doen op de verwerker.

(4) In de interne relatie tussen opdrachtgever en verwerker is de verwerker echter alleen aansprakelijk voor de schade die door de verwerking is veroorzaakt indien hij
    a) niet heeft voldaan aan zijn verplichtingen specifiek opgelegd door de AVG of
    b) heeft gehandeld in strijd met de rechtmatig gegeven instructies van de opdrachtgever of tegen deze instructies in.

(5) Verdere aansprakelijkheidsclaims volgens de algemene wetgeving blijven onaangetast.

§ 18 Schriftelijke vorm clausule

(1) Voor alle wijzigingen van en aanvullingen op deze bijlage en alle componenten daarvan - inclusief eventuele garanties van de verwerker - is een schriftelijke overeenkomst vereist, die ook in een elektronisch formaat (tekstvorm) kan zijn, alsmede de uitdrukkelijke vermelding heeft dat het gaat om een wijziging van of een aanvulling op deze voorwaarden. Dit geldt ook voor het afzien van deze formele vereiste.

§ 19 Salvatorische clausule

(1) In geval van tegenstrijdigheden hebben de bepalingen van deze overeenkomst inzake gegevensbescherming voorrang op de bepalingen van de hoofdovereenkomst.

(2) Indien individuele bepalingen van deze overeenkomst geheel of gedeeltelijk ongeldig of onuitvoerbaar blijken te zijn, of als gevolg van wijzigingen in de wetgeving na het sluiten van de overeenkomst ongeldig of onuitvoerbaar worden, dan blijven de overige bepalingen en de geldigheid van de overeenkomst als geheel onaangetast.

(3) De ongeldige of onuitvoerbare bepaling moet worden vervangen door een geldige en uitvoerbare bepaling die de betekenis en het doel van de ongeldige bepaling zo dicht mogelijk benadert.

(4) Indien de overeenkomst onvolledig blijkt te zijn, worden die bepalingen geacht te zijn overeengekomen, die overeenstemmen met de zin en het doel van de overeenkomst en die zouden zijn overeengekomen indien de partijen ze hadden overwogen.

§ 20 Toepasbaarheid

(1) Deze overeenkomst treedt in werking na ondertekening door de contractpartijen.

(2) Vanaf 25 mei 2018 is de VERORDENING (EU) 2016/679 VAN HET EUROPEES PARLEMENT EN DE RAAD van 27 april 2016 betreffende de bescherming van natuurlijke personen bij de verwerking van persoonlijke gegevens, betreffende het vrije verkeer van gegevens en tot de intrekking van de richtlijn 95/46/EG (Algemene Verordening Gegevensbescherming) van toepassing.

§ 21 Geldende wetgeving en rechtsgebied

(1) De Nederlandse wetgeving is van toepassing.

(2) Het rechtsgebied is de vestigingsplaats van de verwerker.

[Plaats], [DD-MM-JJJJ]	Amsterdam, [DD-MM-JJJJ
[volledige naam AG]	Idiligo B.V.
_____	_____
[Opdrachtgever]	[Verwerker/ opdrachtnemer]

Bijlagen:

Bijlage 1: Technische en organisatorische maatregelen

Bijlage 2: Aanstelling van de functionaris voor gegevensbescherming, contactpersoon en/of vertegenwoordiger binnen de Unie

Bijlage 3: Ingeschakelde onderaannemers

Bijlage 4: Overeengekomen servicelocaties volgens § 7

Bijlage 1

Technisch-organisatorische maatregelen

1. Vertrouwelijkheid (art. 32, lid 1, punten a, b AVG)

Toegangscontrole

Onbevoegde toegang moet worden voorkomen, waarbij de term ruimtelijk moet worden opgevat. Technische en organisatorische maatregelen voor toegangscontrole, met name voor de legitimatie van de bevoegde personen:

- ☒ Vastlegging van bevoegde personen inclusief de omvang van de respectieve bevoegdheden
- ☒ Zorgvuldige selectie van schoonmaakpersoneel
- ☒ Afgifte van toegangspasjes
- ☒ Bestaan van een reglement voor externe personen (begeleiden van de bezoeker door medewerkers, scheiding van ruimtes voor verwerking en openbare ruimtes)
- ☒ Implementatie van belangrijke voorschriften
- ☒ Registratie van inkomende en uitgaande personen

Aanwezigheid van fysieke maatregelen en regelmatige controle ervan:

- ☒ Beveiligde ingang (bijv. afsluitbare deuren, veiligheidssloten)
- ☒ Deurbeveiliging (elektrische deuropener)
- ☒ Inbraakwerende ramen
- ☒ Beveiliging van apparaten tegen diefstal, manipulatie of beschadiging
- ☒ Bewakingsapparatuur (bijv. alarmsysteem, videobewaking)
- ☒ Scheidingssysteem (bijv. draaihek, sluis)
- ☒ Bewakingspersoneel, conciërges
- ☒ Verdeling in verschillende veiligheidszones

Andere:

Toegangscontrole

Het binnendringen van onbevoegden in de IT-systemen en het onrechtmatig gebruik van het systeem moet worden voorkomen.

Technische en organisatorische maatregelen met betrekking tot gebruikersidentificatie en authenticatie:

- ☒ Opstelling en implementatie van een autorisatieconcept
- ☒ Autorisatieconcept voor eindapparaten (computers)
- ☒ Autorisatieconcept voor software/systemen
- ☒ Identificatie- en autorisatiecontrole van een gebruiker
- ☒ Implementatie van een systeem voor het beheren van gebruikersidentiteiten
- ☒ Monitoring van toegangspogingen met reactie op veiligheidsincidenten
- ☒ Vastlegging en controle van toegangsautorisaties
- ☒ Authenticatieprocedure volgens de beschermingsvereisten van de informatie (Classificatie)
- ☒ Versleuteling
- ☐ Externe interfaces blokkeren (USB, enz..)
- ☒ Geschikte wachtwoordbeveiliging (gedragsregels, versleutelde archieven)
- ☒ Speciale beveiligingssoftware (anti-malware, virusscanners, software- en hardware-firewall)
- ☒ Twee-factor-authenticatie
- ☒ Bestaan van voorschriften voor externe personen
- ☐ Toegangsfunctie via token

Andere:

Toegangscontrole

Onbevoegde activiteiten in IT-systemen die buiten de verleende autorisaties vallen, moeten worden voorkomen.

Behoeftegericht ontwerp van het autorisatieconcept en de toegangsrechten, evenals hun monitoring en registratie op basis van:

- ☒ Autorisatie- en rolconcept voor applicaties
- ☒ Implementatie van voorschriften voor toegang- en gebruikersautorisatie
- ☒ Controle van de autorisaties
- ☒ Functiebeperking (functioneel/tijdelijk)
- ☒ Toegangsbeperkingen (volgens 'need-to-know' en 'least privilege')
- ☒ Versleutelde gegevensopslag
- ☒ Registratie van de toegang tot applicaties, met name bij het invoeren, wijzigen en wissen van gegevens
- ☒ Registreren van onbevoegde toegangspogingen
- ☐ Regelmatige evaluatie
- ☒ Incidentgerelateerde evaluatie
- ☒ Implementatie van regelgeving voor het wissen van gegevens
- ☒ Implementatie van voorschriften voor de wissing van opslagmedia (gebruik van papiervernietigers of dienstverleners volgens DIN 66933)
- ☒ Implementatie van voorschriften voor het omgaan met elektronische opslagmedia
- ☒ Integriteitscontrole

Andere:

Scheidingscontrole

Gegevens die voor verschillende doeleinden worden verzameld, moeten afzonderlijk worden verwerkt.

Maatregelen voor de afzonderlijke verwerking (opslag, wijziging, wissing, verzending) van gegevens met verschillende doeleinden:

Capaciteit geschikt voor meerdere soorten cliënteel:

- ☒ Fysieke scheiding
- ☒ Logische cliëntscheiding (op basis van software)
- ☒ Scheiding van productie- en testsystemen
- ☒ Sandboxing
- ☒ Vastlegging van databankrechten
- ☐ Documentatie van de functionele scheiding (Niet van toepassing)
- ☒ Aanwezigheid van richtlijnen en werkinstructies
- ☒ Aanwezigheid van procedurele documentatie
- ☒ Regelmatige controle van het beoogde gebruik van de informatie en IT-systemen

Andere:

Pseudonimisering en versleuteling

De verwerking van persoonlijke gegevens op zodanige wijze dat de gegevens niet meer aan een specifieke betrokkene kunnen worden toegewezen zonder het gebruik van aanvullende informatie, mits deze aanvullende informatie apart wordt bewaard en onderhevig is aan geschikte technische en organisatorische maatregelen:

- [x] Trusted Third Party
- [ ] Blinde handtekening
- [x] Softwarematige versleuteling voor gegevensopslag
- [ ] Hardwarematige versleuteling voor gegevensopslag

Andere:

2. Integriteit (art. 32, lid 1, punt b AVG)

Overdrachtscontrole

Aspecten met betrekking tot de openbaarmaking en overdracht van persoonlijke gegevens moeten worden geregeld: Elektronische verzending, datatransport, transmissiecontrole. Maatregelen voor transport, overdracht en verzending of opslag op datadragers (handmatig of elektronisch) en voor controle achteraf:

Voor elektronische datadragers:

- ☒ Versleuteling van de gegevensoverdracht (bijv.VPN, S/MIME)
- ☒ Elektronische handtekening
- ☒ Implementatie van de registraties van de gegevensoverdracht of doorgave
- ☒ Incidentgerelateerde implementatie van plausibiliteits-, volledigheids- en correctheidscontroles
- ☒ Maatregelen om ongecontroleerde informatie-uitstroom te voorkomen (bijv. deactivering van USB-interfaces, regelmatige controle van de goedgekeurde ontvangers, technische beperking van goedgekeurde ontvangers)
- ☒ Documentatie van de vormen van gegevensoverdracht (bijv. afdruk, datadragers, geautomatiseerde verzending)
- ☒ Doorgifte van gegevens in geanonimiseerde of gepseudonimiseerde vorm
- ☒ Lijst met ontvangers van de gegevens
- ☒ Documentatie van de interfaces en de opvraag- en verzendprogramma's

Voor afdrukken en datadragers:

- ☒ Implementatie van regelmatige bestandscontroles
- ☐ Zorgvuldige selectie van transportpersoneel en -voertuigen (Niet van toepassing)
- ☐ Incidentgerelateerde beveiliging van het transport (bijv. containers, versleuteling van opslagmedia, overdrachtsprotocollen) (Niet van toepassing)

Andere:

Invoercontrole

De traceerbaarheid en documentatie van het gegevensbeheer en het -onderhoud moeten gegarandeerd zijn.

Maatregelen om vervolgens te controleren of en door wie gegevens zijn ingevoerd, gewijzigd of verwijderd (gewist):

- ☒ Registratie van inzendingen en controle van de logboeken
- ☒ Traceerbaarheid van invoer, wijziging en wissing van gegevens via individuele gebruikersnamen (niet gebruikersgroepen)
- ☒ Bewaring van formulieren van waaruit gegevens zijn overgedragen naar geautomatiseerde verwerking
- ☒ Toewijzing van rechten om gegevens in te voeren, te wijzigen en te wissen op basis van een autorisatieconcept
- ☒ Organisatorisch vastgelegde verantwoordelijkheden voor de invoer

Andere:

3. Beschikbaarheid en belastbaarheid (art. 32, lid 1, punten b, c AVG)

Beschikbaarheidscontrole

De gegevens moeten worden beschermd tegen onbedoelde vernietiging of verlies.

Maatregelen voor gegevensback-up (fysiek/logisch):

☒ Regelmatige controle van de systeemstatus (monitoring)

☒ Herstel op korte termijn van de normale systeemstatus

Back-up en herstartconcept (regelmatige back-ups van de gegevens):

☐ offline ☒ online ☒ onsite ☐ offsite ☐

☒ Concept voor gegevensarchivering

☒ Bestaan van een noodplan (Business Continuity, Disaster Recovery)

☒ Regelmatige tests van het noodplan

☒ Bestaan van redundante IT-systemen (bijv. server, opslag)

☒ Repliceerbaarheid van virtuele machines

☒ Functionele, fysieke beschermingsmiddelen (brandbeveiliging, energie: noodstroomvoeding, airconditioning)

☒ Meldingskanalen en noodplannen

Andere:

Belastbaarheidscontrole

De verwerking van de gegevens moet tolerant zijn voor storingen en fouten.

- ☒ Anti-virus/anti-malware/anti-ransomware
- ☒ Aanwezigheid van ruime netwerkcapaciteit
- ☒ Beveiligde hardware tegen vooral DoS- en DDoS-aanvallen
- ☐ IDS/IPS
- ☒ geschikte systeemarchitectuur/DMZ
- ☒ Firewall

4. Procedures voor regelmatige controle, beoordeling en evaluatie

(art. 32, lid 1, punt d AVG; art. 25, lid 1 AVG)

☒ Schriftelijke voorschriften van de verantwoordelijkheden voor gegevensbescherming

☒ Schriftelijke voorschriften van de verantwoordelijkheden voor informatiebeveiliging

☒ Bestaan van een adequaat informatiebeveiligingsbeheer

☒ Bestaan van een adequaat Incident Response beheer

☒ Implementatie van een informatieclassificatie

☒ Regelmatige scholing en sensibilisatie van medewerkers en managers

☒ Gebruiksvriendelijke standaardinstellingen voor gegevensbescherming (art. 25, lid 2 AVG);

Ordercontrole om verwerking conform de instructies te garanderen:

☒ Strikte naleving van de gemaakte afspraken en hun betreffende controles

☒ Concept van de wijze waarop de regelmatige controle van de opdrachtsprocedure wordt uitgevoerd (bijv. indiening van zelfevaluaties, indiening van overeenkomsten met onderaannemers, implementatie van controles bij onderaannemers door de opdrachtnemer)

☒ Geen verwerking van gegevens in de zin van art. 28 AVG zonder overeenkomstige instructies van de opdrachtgever, bijv. op basis van: duidelijke opmaak van de overeenkomst, geformaliseerd orderbeheer, strikte selectie van de dienstverlener, verplichting om vooraf te overtuigen, nacontroles.

Andere:

Bijlage 2

Aanstelling van de functionaris voor gegevensbescherming, contactpersoon of vertegenwoordiger binnen de Unie conform § 16 OV-overeenkomst

De verwerker benoemt:

Als functionaris voor gegevensbescherming de heer Dr. Timo Hoffmann

Adres: Eckweg 1, 78048 Villingen-Schwenningen

E-mail: timo.hoffmann@hub24.de

Als contactpersoon de heer Frank Korthouwer

Adres: Kabelweg 57, 1014 BA Amsterdam

Tel.: +31 23 3000000

E-mail: frank.korthouwer@idiligo.com

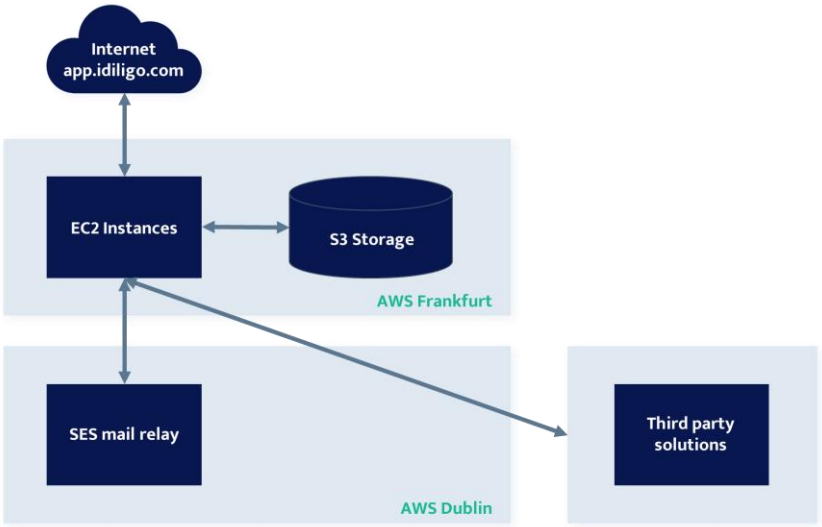
Bijlage 3

Onderaannemersrelatie met de verwerker op het moment van de gunning van de opdracht

Naam van de onderaannemer	Beschrijving van de deelprestaties	Plaats van de geleverde diensten
Amazon (AWS)	Opslag van gegevens in de Amazon S3-opslag. Zowel EC2 als S3	Frankfurt, Duitsland
Amazon (AWS)	SES mail-relay-functie	Dublin, Ierland
Digital Intelligence	Ontwikkeling van de Idiligo-applicatie	Amsterdam, Nederland
The Rocket Science Group LLC d/b/a Mailchimp	Klantinformatie per e-mail	Derde landen, EU
Exact	Factuurverzending	EU
Intelligent Solution Services AG	Digitale handtekening	Stuttgart, Duitsland

Beveiligingsmanagement & architectuur

- De Elastic Compute Cloud (EC2) van Amazon biedt een functie genaamd Security Groups, die vergelijkbaar is met een inkomende netwerkfirewall, waarin Idiligo de protocollen, poorten en bron-IP-bereiken specificeert die de EC2-instanties mogen bereiken.
  Opslag & back-ups
- Documenten die zijn geüpload of gegenereerd voor gebruik tijdens interactieve Idiligo-vergaderingen, worden in S3 opgeslagen. De gegevens worden versleuteld opgeslagen met behulp van AWS Key Management Service (KMS).
  Idiligo implementeert een dagelijkse back-up van klantspecifieke informatie met een maximale geschiedenis van 8 dagen in een aparte Amazon S3-omgeving.



Bijlage 4

Overeengekomen servicelocaties volgens § 7 van de overeenkomst

Naam en adres van de verwerker	**Naam en adres van de onderaannemer**	**Plaats van de geleverde diensten**
Idiligo B.V. Kabelweg 57, 1014 BA Amsterdam, Nederland	Amazon (AWS) Frankfurt	Duitsland