VERWERKERSOVEREENKOMST

Therp BV, een besloten vennootschap met beperkte aansprakelijkheid, gevestigd te Amsterdam, kantoorhoudende te 1053 NJ aan de Jacob van Lennepkade 334k hierbij rechtsgeldig vertegenwoordigd door Anne Sedee, Algemeen Directeur, hierna te noemen: “Verwerker”,

Verwerkingsverantwoordelijke, NAAM kantoorhoudende aan ADRES, hierbij rechtsgeldig vertegenwoordigd door NAAM2, hierna te noemen: “Verwerkingsverantwoordelijke”,

Gezamenlijk hierna ook te noemen “Partijen”,

Overwegende dat:

- Verwerkingsverantwoordelijke gebruik wil maken van de diensten van Verwerker;
- Partijen hiertoe een overeenkomst hebben getekend ten aanzien van de door Verwerker te verrichten diensten m.b.t. ontwikkeling, implementatie en beheer van op Odoo gebaseerde webapplicaties (hierna: “Overeenkomst”);
- Verwerker in het kader van de Overeenkomst Persoonsgegevens in de zin van de Algemene verordening gegevensbescherming (“AVG”) (hierna: “persoonsgegevens”) zal verwerken ten behoeve van Verwerkingsverantwoordelijke;
- De data van Verwerkingsverantwoordelijke en persoonsgegevens van Betrokkenen, zo goed mogelijk beschermd dienen te worden. Een Betrokkene is elke identificeerbare natuurlijke persoon op wie een persoonsgegeven betrekking heeft.
- Partijen - mede ter uitvoering van het bepaalde in artikel 28 lid 3 AVG - in de onderhavige aanvullende overeenkomst (hierna: “Verwerkersovereenkomst”) een aantal voorwaarden wensen vast te leggen die van toepassing zijn op hun relatie in verband met de genoemde activiteiten in opdracht van en ten behoeve van Verwerkingsverantwoordelijke;
- De in de onderhavige overeenkomst gehanteerde definities van “Verwerker” “Verwerkingsverantwoordelijke” , “Persoonsgegevens”, “verwerken” en “verwerking” in overeenstemming zijn met van toepassing zijnde definities zoals gehanteerd in artikel 4 AVG;
- Dat de AVG van toepassing is en Partijen de intentie hebben met de onderhavige Verwerkersovereenkomst aan de toepasselijke wetgeving te voldoen.

Verklaren te zijn overeengekomen als volgt:

ARTIKEL 1 ALGEMEEN

1. Alle data en persoonsgegevens in de databases van Verwerkingsverantwoordelijke staan onder volledige controle van Verwerkingsverantwoordelijke zowel gedurende als na beëindiging van Overeenkomst met Verwerker.
2. Ook Verwerkingsverantwoordelijke staat er tegenover Verwerker voor in dat hij conform de AVG handelt, dat hij zijn systemen en infrastructuur te allen tijde adequaat beveiligt en dat de inhoud, het gebruik en/of de verwerking van de Persoonsgegevens niet onrechtmatig zijn en geen inbreuk maken op enig recht van een derde.
3. Deze Verwerkersovereenkomst, en de daarin opgenomen beveiligingsmaatregelen, kunnen van tijd tot tijd door Verwerker worden aangepast indien dat naar zijn oordeel noodzakelijk is om een passend beveiligingsniveau te blijven bieden in veranderende omstandigheden.
4. Verwerker zal Verwerkingsverantwoordelijke van aanpassingen op de hoogte stellen. Indien Verwerkingsverantwoordelijke in redelijkheid niet akkoord kan gaan met de aanpassingen, is Verwerkingsverantwoordelijke gerechtigd binnen 30 dagen na kennisgeving van de aanpassingen de verwerkersovereenkomst schriftelijk gemotiveerd op te zeggen.

ARTIKEL 2 BEVEILIGING

1. Verwerkingsverantwoordelijke stelt enkel Persoonsgegevens aan Verwerker ter beschikking voor verwerking, indien Verwerkingsverantwoordelijke zich er van heeft verzekerd dat de vereiste beveiligingsmaatregelen zijn getroffen, welke mede gelet op het bepaalde in artikel 32 AVG een passend beschermingsniveau garanderen, gelet op de stand van de techniek en de kosten van de tenuitvoerlegging, gelet op de risico’s die de verwerking en de aard van de te beschermen gegevens met zich meebrengen, van welke beveiligingsmaatregelen een overzicht is opgenomen in Bijlage 1-B.
2. Verwerkingsverantwoordelijke is gerechtigd de maatregelen en de naleving van de op Verwerker rustende verplichtingen te controleren, op voorwaarde dat Verwerkingsverantwoordelijke Verwerker daarvan vijf (5) werkdagen van tevoren op de hoogte stelt en op voorwaarde dat Verwerkingsverantwoordelijke bij de inspectie de redelijke aanwijzingen van Verwerker opvolgt en de inspectie de bedrijfsvoering van Verwerker niet onredelijk verstoort.
3. Als Verwerkingsverantwoordelijke oordeelt dat Verwerker niet afdoende garanties biedt, kan Verwerkingsverantwoordelijke aanvullende maatregelen voorstellen. Verwerker zal, waar mogelijk, zijn medewerking verlenen aan redelijke verzoeken. Pas nadat de door Verwerkingsverantwoordelijke gewenste gewijzigde beveiligingsmaatregelen schriftelijk zijn overeengekomen en ondertekend door Partijen, heeft Verwerker de verplichting deze beveiligingsmaatregelen daadwerkelijk te implementeren. Verwerker kan de kosten verband houdende met de op verzoek van Verwerkingsverantwoordelijke doorgevoerde wijzigingen in rekening brengen bij Verwerkingsverantwoordelijke.
4. In geval Verwerker kennis heeft genomen van een "Datalek", dit is een beveiligingsincident waarbij Persoonsgegevens, die de Verwerker namens de Verwerkingsverantwoordelijke beheert, mogelijk onbruikbaar zijn geworden of onbedoeld toegankelijk waren voor derden, zoals omschreven in artikel 4 lid 12 AVG, zal Verwerker Verwerkingsverantwoordelijke zonder onredelijke vertraging, en in ieder geval binnen 24 (vierentwintig) uur nadat het Datalek ter kennis van Verwerker is gekomen, informeren, met daarbij tenminste alle informatie en op de wijze zoals aangegeven in Bijlage 1-D.
5. Indien zich, ondanks het feit dat Verwerker maatregelen zoals afgestemd met Verwerkingsverantwoordelijke heeft doorgevoerd, een Datalek voordoet, kan Verwerkingsverantwoordelijke de Verwerker niet aansprakelijk houden voor enige door Verwerkingsverantwoordelijke of derden als gevolg hiervan geleden schade, zoals verder uitgewerkt in Artikel 7 Aansprakelijkheid.

ARTIKEL 3 DATALEK / BIJSTAND VERLENEN

1. Verwerker zal, ingeval van een Datalek, indien gewenst en zover dat mogelijk is, bijstand verlenen aan Verwerkingsverantwoordelijke opdat deze
   – kan voldoen aan verzoeken van Betrokkenen;
   – invulling kan geven aan de rechten van Betrokkenen;
   – de verplichtingen uit hoofde van de artikelen 32 tot en met 36 AVG kan nakomen;
   – kan voldoen aan verzoeken van de bevoegde toezichthouder;
2. Verwerker kan eventuele kosten die hij maakt in het kader van dit artikel in rekening brengen bij Verwerkingsverantwoordelijke.

ARTIKEL 4 DERDE LANDEN

1. Verwerker slaat geen Persoonsgegevens op in derde landen. Derde landen zijn alle landen buiten de Europese Unie en Europese Economische Ruimte of internationale organisaties.
2. Hoewel Verwerker samenwerkt met programmeurs van bedrijven in derde landen, kunnen zij niet bij Persoonsgegevens of toegangs-data voor databases van Verwerkingsverantwoordelijke; verwerker geeft hen dergelijke gegevens niet door. Verwerker geeft alleen dergelijke gegevens door met uitdrukkelijke schriftelijke toestemming van Verwerkingsverantwoordelijke én als dat op grond van de toepasselijke (Europese) privacyregelgeving is toegestaan, bijvoorbeeld omdat het betreffende land een passend beschermingsniveau biedt of gebruik wordt gemaakt van een daartoe bestemd ongewijzigd modelcontract, goedgekeurd door de Europese Commissie.

ARTIKEL 5 SUB-VERWERKERS

1. Verwerker heeft Sub-verwerkers ingeschakeld zoals beschreven in Bijlage 1-D
2. Verwerker draagt ervoor zorg dat Sub-verwerkers zich aan eenzelfde beveiligingsniveau committeren ten aanzien van de bescherming van de Persoonsgegevens als het beveiligingsniveau waaraan Verwerker jegens Verwerkingsverantwoordelijke is gebonden.

ARTIKEL 6 GEHEIMHOUDING

1. Toegang tot persoonsgegevens, toegangs- en/of identificatiecodes, certificaten en alle andere data die invulling geeft aan deze Verwerkersovereenkomst, is beperkt tot de medewerkers bij Verwerker of Sub-verwerker waarvoor toegang gezien hun functie noodzakelijk is. Al deze medewerkers hebben standaard een verplichting tot geheimhouding, waaronder geheimhouding van persoonsgegevens.
2. Verwerker is alleen gerechtigd de Persoonsgegevens te verstrekken aan derden, indien en voor zover verstrekking noodzakelijk is ingevolge een rechterlijke uitspraak, een wettelijk voorschrift of op basis van een bevoegd gegeven bevel van een overheidsinstantie.
3. Als Overeenkomst wordt beëindigd kan Verwerkingsverantwoordelijke een kopie van de database meenemen of een export maken van de persoonsgegevens vanuit de software.
4. Tenzij schriftelijk anders overeengekomen, worden na beëindiging van de overeenkomst de persoonsgegevens die voor de Verwerkingsverantwoordelijke werden verwerkt, en alle bestaande kopieën, door Verwerker op zodanige wijze verwijderd dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn.
5. Verwerker kan eventuele kosten die hij maakt in het kader van dit artikel in rekening brengen bij Verwerkingsverantwoordelijke.

ARTIKEL 7 AANSPRAKELIJKHEID

1. Indien Verwerker aansprakelijk is jegens Verwerkingsverantwoordelijke voor schade uit welke hoofde dan ook, is Verwerker alleen aansprakelijk voor directe schade die Verwerkingsverantwoordelijke lijdt als gevolg van een aan Verwerker toerekenbare tekortkoming en/of onrechtmatige daad.
2. De totale aansprakelijkheid onder de Overeenkomst, inclusief de Verwerkersovereenkomst, of overtreding door Verwerker en/of sub-verwerker(s) van de toepasselijke (Europese) privacyregelgeving, zal nooit meer bedragen dan de som van de ontvangen bedragen door Verwerker van Verwerkingsverantwoordelijke van de afgelopen 6 maanden met een maximum van € 50.000.
3. Verwerker is nooit aansprakelijk voor gevolgschade, waaronder mede begrepen zuivere vermogensschade, gederfde winst, en immateriële schade. In het bijzonder is Verwerker niet aansprakelijk voor schade in verband met en/of als gevolg van:
   a) beëindiging of wijziging van de geleverde dienst;
   b) communicatiegebreken in verband met hardware-, software-, netwerk- of andere computerproblemen;
   c) het gebruik van door Verwerkingsverantwoordelijke voorgeschreven gegevens of databestanden;
   d) verlies, verminking of vernietiging van gegevens of databestanden; en/of,
   e) ontoegankelijkheid van de dienst van Verwerker;
   f) reputatieschade.
4. Voorwaarde voor het ontstaan van enig recht op schadevergoeding is dat Verwerkingsverantwoordelijke de schade zo spoedig mogelijk na het ontstaan daarvan schriftelijk bij Verwerker meldt. Tenzij het oplossen van de tekortkoming blijvend onmogelijk is, ontstaat aansprakelijkheid van Verwerker daarbij alleen indien een redelijke termijn ter zuivering van de tekortkoming wordt gesteld, en Verwerker ook na die termijn toerekenbaar tekort blijft schieten in de nakoming van haar verplichtingen uit de verwerkersovereenkomst. De ingebrekestelling dient een zo volledig en gedetailleerd mogelijke omschrijving van de tekortkoming te bevatten, zodat Verwerker in staat is adequaat te reageren. Ieder vordering tot schadevergoeding jegens Verwerker vervalt door het enkele verloop van zes (6) maanden na het ontstaan van de vordering.
5. Verwerkingsverantwoordelijke vrijwaart Verwerker voor aanspraken van derden (met name Betrokkenen) en de eventuele schade als gevolg daarvan, gebaseerd op niet naleving van voorschriften bij of krachtens de AVG en/of overige wet en regelgeving ter zake en/of deze Verwerkersovereenkomst.
6. Beperkingen van de aansprakelijkheid opgenomen in deze Verwerkersovereenkomst komen te vervallen indien en voor zover de schade het gevolg is van opzet of bewuste roekeloosheid van Verwerker.

ARTIKEL 8 OVERIG

1. Op de Verwerkersovereenkomst is Nederlands recht van toepassing.
2. Geschillen tussen Verwerkingsverantwoordelijke en Verwerker worden uitsluitend voorgelegd aan de bevoegde rechter in het arrondissement te Amsterdam.

BIJLAGE 1

A DOELEINDEN VERWERKING PERSOONSGEGEVENS

Met haar Odoo oplossingen wil Verwerker opdrachtgevers helpen de processen in hun bedrijf of organisatie zo goed mogelijk te ondersteunen. Of het nu gaat om handig de inkopen en verkopen te verwerken, contracten van vrijwilligers of medewerkers te beheren, projecten te monitoren, campagnes te organiseren, op vragen of issues te reageren, sociale impact te realiseren of inschrijvingen voor evenementen te verwerken, de processen bij de Verwerkingsverantwoordelijke zijn altijd leidend. Odoo is onder andere geschikt voor de verwerking van:

- Contactgegevens van klanten, leveranciers, leden, achterban, vrijwilligers, donateurs, deelnemers, medewerkers;
- Voorkeur communicatiekanalen;
- Vastleggen en analyseren van transacties en interesses;
- Contracten en aanwezigheid van personeel of vrijwilligers;
- Inkoop en Verkoop van producten en diensten;
- Incasso en betalingen;
- Project- , evenement,- of campagneadministratie.

Bij onze oplossingen kunnen dus ook bijzondere persoonsgegevens worden verwerkt. Verwerken van deze bijzondere persoonsgegevens, de duur van de opslag, ook met onze oplossingen en dienstverlening, is en blijft echter ter eigen beoordeling van Verwerkingsverantwoordelijke.

B BEVEILIGING

Voor Verwerker is informatiebeveiliging: “De doeltreffende bescherming van alle als vertrouwelijk geclassificeerde informatie door een samenhangend geheel van passende maatregelen, die zijn gericht op het borgen van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie”. Verwerker hanteert een proactief data protectie beleid, dat erop is gericht om de data van onze klanten, en persoonsgegevens van Betrokkenen, zo goed mogelijk te beschermen. Risico’s worden blijvend in kaart gebracht waarbij op basis van de risicobeoordeling maatregelen worden geformuleerd. De volgende technische en organisatorische beveiligingsmaatregelen zijn getroffen:

- Toegangscontrole, gebruik makend van wachtwoorden en versleuteling;
- Toegang naar implementaties van Verwerkingsverantwoordelijke alleen voor project-deelnemers;
- Toewijzen van verantwoordelijkheden m.b.t. informatiebeveiliging;
- Volgen van relevante ontwikkelingen m.b.t. beveiliging van Odoo en de onderliggende platformen en technologieën;
- Beveiligingsbewustzijn van medewerkers hooghouden;
- Steekproefsgewijze controle op naleving beleid;
- Beveiliging van netwerkverbindingen via versleuteling en toegangscodes versleuteld opslaan.
- Een beveiligd intern netwerk;
- Monitoring van systemen;
- Direct ingrijpen bij verdachte incidenten, ook als dit een onderbreking van de bedrijfsprocessen van Verwerkingsverantwoordelijke betekent;
- Geen persoonsgegevens op de eigen laptop;
- Versleutelde Back-ups.

C DATALEK

Verwerker kan niet garanderen dat de beveiligingsmaatregelen onder alle omstandigheden doeltreffend zijn. Hier staat beschreven hoe en wanneer Verwerker de Verwerkingsverantwoordelijke zal informeren over Beveiligingsincidenten en Datalekken. Een Datalek is een beveiligingsincident waarbij Persoonsgegevens, die de Verwerker namens de Verwerkingsverantwoordelijke beheert, mogelijk onbruikbaar zijn geworden of onbedoeld toegankelijk waren voor derden, zoals omschreven in artikel 4 sub 12 AVG. Het gaat om gegevens die te koppelen zijn aan personen, zoals, maar niet beperkt tot, namen, adressen, telefoonnummers, mailadressen, login gegevens, cookies, IP adressen of identificerende gegevens van computers of telefoons. Verwerker zal Verwerkingsverantwoordelijke desgewenst ondersteunen bij het meldproces.

Een Beveiligingsincident zal zo spoedig mogelijk, doch uiterlijk binnen 24 uur, aan Verwerkingsverantwoordelijke gemeld worden. Onderstaande vragen zullen in de e-mail beantwoord worden. Deze vragen zijn gelijk aan de informatie die aan de Autoriteit Persoonsgegevens moet worden verstrekt.

1. Een samenvatting van het beveiligingslek/beveiligingsincident/datalek:
Wat is er gebeurd? Hier wordt ook de naam van het betrokken systeem gemeld.
2. Betrokken persoonsgegevens bij het beveiligingsincident
Ieder tot een persoon te herleiden gegeven, zoals, maar niet beperkt tot, naam, adres, e-mailadres, IP-nummer, Burgerservicenummer en pasfoto.
3. Het aantal personen waarvan de persoonsgegevens betrokken zijn bij het incident
Een minimum en maximum aantal personen.
4. Omschrijving van de groep personen om wiens gegevens het gaat
Met bijzondere aandacht voor gegevens van kwetsbare groepen.
5. Bekendheid van de contactgegevens van de betrokken personen
Kan Verwerkingsverantwoordelijke de getroffen personen bereiken, indien nodig?
6. De oorzaak van het beveiligingsincident
7. De getroffen maatregelen om het datalek te dichten en herhaling te voorkomen
8. In welke periode het beveiligingsincident heeft plaatsgevonden
9. Wijzen op de mogelijke gevolgen als Persoonsgegevens in verkeerde handen vallen
10. Contactgegevens contactpersoon, waar kan de Verwerkingsverantwoordelijke met vragen terecht

De Verwerker blijft de Verwerkingsverantwoordelijke tevens op de hoogte houden van verdere ontwikkelingen. Wel of niet melden bij de Autoriteit Persoonsgegevens (AP) de toezichthoudende autoriteit, zoals omschreven in artikel 4, sub 21 AVG, blijft te allen tijde de verantwoordelijkheid van de Verwerkingsverantwoordelijke. Verwerker is niet verplicht tot het melden van inbreuken in verband met persoonsgegevens aan de AP en/of de Betrokkene.

D SUB-VERWERKERS

Voor het Verwerken van data maakt Verwerker voor sommige Verwerkingsverantwoordelijken gebruik van Sub-verwerkers. Onze partner SunflowerIT (KVK 60902922) voert grotendeels dezelfde werkzaamheden uit als Verwerker. Verwerker draagt ervoor zorg dat deze Sub-verwerker zich aan eenzelfde beveiligingsniveau committeert ten aanzien van de bescherming van de Persoonsgegevens als het beveiligingsniveau waaraan Verwerker jegens Verwerkingsverantwoordelijke is gebonden.

Zowel Verwerker als Sub-verwerker werken met programmeurs van bedrijven in derde landen. Zij kunnen niet bij Persoonsgegevens of toegangs-data voor databases van Verwerkingsverantwoordelijke; verwerker geeft hen dergelijke gegevens niet door. Verwerker kan alleen dergelijke gegevens doorgeven met uitdrukkelijke schriftelijke toestemming van Verwerkingsverantwoordelijke én als dat op grond van de toepasselijke (Europese) privacyregelgeving is toegestaan.

Verwerker zal Verwerkingsverantwoordelijke informeren over een wijziging in de door de Verwerker ingeschakelde Subverwerkers. Verwerkingsverantwoordelijke heeft het recht bezwaar te maken tegen voornoemde wijziging.

Voor het hosten van databases maakt Verwerker voor sommige Verwerkingsverantwoordelijken, gebruik van de Sub-verwerkers. In deze situatie draagt Verwerker ervoor zorg dat Subverwerkers zich aan eenzelfde beveiligingsniveau committeren ten aanzien van de bescherming van de Persoonsgegevens als het beveiligingsniveau waaraan Verwerker jegens Verwerkingsverantwoordelijke is gebonden. Deze verantwoordelijkheid geldt niet voor Verwerkingsverantwoordelijken die zelf hosten of databases in eigen beheer hebben. Onze Subverwerkers zijn:

Hosting providers	Certificeringen	Meer informatie
Tilaa	ISO 9001 + ISO 27001 + ISAE 3402 + NEN 7510 + PCI DSS	https://www.tilaa.com/nl/stabiel-en-veilig
TransIP	ISO 9001 + ISO 27001 + ISO 14001 + NEN 7510 + PCI DSS	https://www.transip.nl/knowledgebase/artikel