VERWERKINGSOVEREENKOMST

De ondergetekenden:

1. _____**,** gevestigd te _____,, bij de Kamer van Koophandel geregistreerd onder nummer _____, verder te noemen "Verwerkingsverantwoordelijke", enerzijds,

en

2. **Mach3builders B.V.,** gevestigd te Barendrecht, bij de Kamer van Koophandel geregistreerd onder nummer 52909840, verder te noemen "Verwerker", anderzijds,

Hierna gezamenlijk te noemen 'Partijen'

OVERWEGINGEN:

- Partijen zijn in de Hoofdovereenkomst overeen gekomen dat Verwerker bepaalde diensten zal leveren aan Verwerkingsverantwoordelijke op het gebied van website-ontwikkeling en/of –hosting.
- Verwerker zal, in het kader van de Hoofdovereenkomst, in opdracht van Verwerkingsverantwoordelijke persoonsgegevens (hierna: "Persoonsgegevens") verwerken in de zin van de Algemene Verordening Gegevensbescherming (Verordening 2016/679/EU; hierna: de AVG);
- Verwerkingsverantwoordelijke kan, afhankelijk van de situatie, aangemerkt worden als Verwerkingsverantwoordelijke dan wel als een afzonderlijke verwerker (in de zin van de AVG) ten behoeve van een Verwerkingsverantwoordelijke. In laatst vermeld geval fungeert Verwerker als Sub-Verwerker;
- Partijen – mede ter uitvoering van het bepaalde artikel 28 van de AVG – in de onderhavige Verwerkingsovereenkomst een aantal voorwaarden wensen vast te leggen die van toepassing zijn op hun relatie in verband met de vermelde verwerkingsdiensten van Verwerker.

PARTIJEN VERKLAREN TE ZIJN OVEREENGEKOMEN ALS VOLGT:

1. DEFINITIES

1.1 Betrokkene:
De natuurlijke persoon op wie een Persoonsgegeven betrekking heeft.

1.2 Verwerker:
De natuurlijke persoon of rechtspersoon die ten behoeve van de Verwerkingsverantwoordelijke (al dan niet via een andere Verwerker) Persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.

1.3 Verwerkingsovereenkomst:
Deze overeenkomst tussen Verwerkingsverantwoordelijke en Verwerker met als onderwerp het verwerken van Persoonsgegevens, inclusief alle documenten waarnaar verwezen wordt en die de nadere rechten en verplichtingen van Partijen uiteenzetten.

1.4 Datalek:
Een inbreuk op beveiligingsmaatregelen die erop zijn gericht Persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige Verwerking, alsmede enig incident of enige gebeurtenis waarbij verlies of onrechtmatige Verwerking van Persoonsgegevens plaatsvindt dan wel zou kunnen plaatsvinden.

1.5 Hoofdovereenkomst:
De overeenkomst die Verwerkingsverantwoordelijke en Verwerker zijn aangegaan ter levering van diensten door Verwerker en waaruit verwerking van Persoonsgegevens voortvloeit.

1.6 Persoonsgegeven:
Elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon.

1.7 Sub-Verwerker:
De natuurlijke persoon of rechtspersoon die een Verwerker bijstaat in het Verwerken van

Persoonsgegevens ten behoeve van Verwerkingsverantwoordelijke.

1.8 Verwerkingsverantwoordelijke:
De natuurlijke persoon, rechtspersoon of ieder ander die, of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van Persoonsgegevens vaststelt.

1.9 Verwerking van Persoonsgegevens:
Elke handeling of elk geheel van handelingen met betrekking tot Persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens.

1.10 Alle van de hierboven gebruikte woorden en termen in het enkelvoud hebben dezelfde betekenis als in het meervoud en vice versa.

1.11 De aanduidingen boven de artikelen van deze Verwerkingsovereenkomst hebben uitsluitend tot doel de leesbaarheid van de Verwerkingsovereenkomst te vergroten. De inhoud en strekking van het onder een bepaalde aanduiding opgenomen artikel beperken zich derhalve niet tot die aanduiding.

2. VERWERKING VAN PERSOONSGEGEVENS

2.1 De Verwerkingsverantwoordelijke stelt het doel en de middelen voor de verwerking van Persoonsgegevens vast. Dit doel is opgenomen in Appendix 1.

2.2 Verwerkingsverantwoordelijke laat Persoonsgegevens verwerken door Verwerker. Een overzicht van de categorieën Persoonsgegevens die Verwerker kan verwerken, wordt opgenomen in Appendix 1. Verwerker verwerkt deze Persoonsgegevens uitsluitend ter uitvoering van de Hoofdovereenkomst, deze Verwerkingsovereenkomst, en de door de Verwerkingsverantwoordelijke gegeven schriftelijke instructies. Verwerker zal de Persoonsgegevens onder geen enkele omstandigheid voor eigen doeleinden gebruiken, behoudens andersluidende wettelijke verplichtingen.

2.3 Verwerker mag in het kader van de Verwerkersovereenkomst gebruik maken van een derde, mits Verwerkingsverantwoordelijke hiervoor voorafgaande schriftelijke toestemming heeft verleend. De Verwerkingsverantwoordelijke kan de inschakeling van derden zonder opgave van redenen verbieden.

2.4 Verwerker zorgt er onvoorwaardelijk voor dat deze derden schriftelijk dezelfde plichten op zich nemen als tussen Verwerkingsverantwoordelijke en Verwerker zijn overeengekomen. Verwerker staat in voor een correcte naleving van deze plichten door deze derden en is bij fouten van deze derden zelf jegens Verwerkingsverantwoordelijke aansprakelijk voor alle schade alsof hij zelf de fout(en) heeft begaan. Verwerkingsverantwoordelijke geeft daarnaast toestemming voor het inschakelen van de in Appendix 2 genoemde sub-Verwerkers.

2.5 Verwerker zal de Persoonsgegevens alleen verwerken door hemzelf of laten verwerken door derden in landen binnen de Europese Economische Ruimte (“EER”) dan wel in landen welke een waarborg tot een passend beschermingsniveau bieden conform artikel 45 AVG (Adequaatheidsbesluit).

2.6 Verwerker zal Verwerkingsverantwoordelijke indien nodig bijstand verlenen bij het nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36 van de AVG.

2.7 In het geval dat een betrokkene een verzoek tot uitoefening van zijn/haar wettelijke rechten richt aan Verwerker, zal Verwerker het verzoek doorsturen aan Verwerkings-verantwoordelijke en de betrokkene hiervan op de hoogte stellen. Verwerkingsverantwoordelijke zal het verzoek vervolgens verder zelfstandig afhandelen. Indien blijkt dat de Verwerkingsverantwoordelijke hulp benodigd heeft van de Verwerker voor de uitvoering van een verzoek van een betrokkene, dan is Verwerker verplicht om zijn medewerking te verlenen.

2.8 Verwerker zal Verwerkingsverantwoordelijke alle informatie ter beschikking stellen die nodig is om de nakoming van deze Verwerkingsovereenkomst aan te tonen. Daartoe zal Verwerker met name medewerking verlenen aan audits, waaronder inspecties, door Verwerkingsverantwoordelijke of een door Verwerkingsverantwoordelijke gemachtigde controleur. De kosten van dergelijke audits worden gedragen door Verwerkingsverantwoordelijke. Indien uit de audit volgt dat Verwerker enige verplichting uit de Verwerkingsovereenkomst niet is nagekomen, neemt Verwerker de maatregelen die redelijkerwijs

nodig zijn om alsnog aan de desbetreffende verplichting(en) te voldoen.

2.9 Verwerkingsverantwoordelijke staat ervoor in dat de verwerking van Persoonsgegevens zoals opgedragen aan Verwerker, niet in strijd is met regelgeving betreffende bescherming van Persoonsgegevens en niet onrechtmatig is. Indien Verwerkingsverantwoordelijke zelf een verwerker is, staat Verwerkingsverantwoordelijke ervoor in de vereiste toestemming te hebben om Verwerker in te schakelen, en Verwerker toe te staan Sub-Verwerkers in te schakelen. Verwerkingsverantwoordelijke vrijwaart Verwerker voor alle aanspraken van derden, inclusief toezichthouders, die verband houden met het in dit artikel 2.9 bepaalde.

3. BEVEILIGING

3.1 Verwerker treft passende technische en organisatorische maatregelen om de Persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen Persoonsgegevens met zich meebrengen.

3.2 De bij het aangaan van de Verwerkingsovereenkomst genomen maatregelen als bedoeld in artikel 3.1 worden weergegeven in Appendix 2. Verwerkingsverantwoordelijke erkent dat Verwerker met de in Appendix 2 vermelde maatregelen voldoet aan de verplichting bedoeld in artikel 3.1.

3.3 Indien Verwerkingsverantwoordelijke wenst dat Verwerker de maatregelen als bedoeld in artikel 3.1 actualiseert omdat dit naar het oordeel van Verwerkingsverantwoordelijke nodig is om een passend beveiligingsniveau als bedoeld in artikel 3.1 te blijven garanderen, is Verwerker gerechtigd de overeengekomen prijzen met Verwerkingsverantwoordelijke te verhogen. Partijen zullen daaromtrent in overleg treden.

4. DATALEKKEN

4.1 Verwerker zal enig Datalek na ontdekking hiervan door Verwerker, zonder onredelijke vertraging en in ieder geval binnen 24 uur rapporteren aan Verwerkingsverantwoordelijke, zodat laatstgenoemde vervolgens binnen 72 uur de toezichthouder kan informeren. Verwerker vermeldt daarbij in ieder geval de volgende gegevens:

a) De (vermoedelijke) oorzaak van het Datalek;
b) de (vooralsnog bekende en/of te verwachten) gevolgen van het Datalek;
c) locatiegegevens van het Datalek;
d) de eventuele onbevoegde ontvangers van de Persoonsgegevens en alle beschikbare informatie over hen;
e) voorstellen voor maatregelen ter beperking van de schade;
f) eventuele andere gegevens indien Verwerkingsverantwoordelijke daarom verzoekt.

4.2 Verwerker zal op verzoek van Verwerkingsverantwoordelijke meewerken aan het adequaat informeren van Betrokkenen of de toezichthoudende instanties over het Datalek, en zich ter zake beschikbaar houden voor overleg met Verwerkingsverantwoordelijke.

4.3 Verwerkingsverantwoordelijke en Verwerker betrachten strikte geheimhouding jegens ieder ander dan elkaar omtrent het Datalek, eventuele vrees voor een Datalek en verdere gerelateerde zaken, behoudens andersluidende verplichtingen op grond van Unierecht of Nederlands recht.

5. GEHEIMHOUDING

5.1 Partijen zijn zich ervan bewust dat Persoonsgegevens kwalificeren als confidentiële informatie en zijn gehouden zijn tot geheimhouding van de Persoonsgegevens. Persoonsgegevens mogen slechts gebruikt worden ter uitvoering van de Hoofdovereenkomst en deze Verwerkingsovereenkomst.

5.2 Partijen zullen de Persoonsgegevens niet aan anderen ter beschikking stellen dan zijn eigen werknemers en/of derden die een legitieme reden hebben tot inzage daarvan. Verwerker zal waarborgen dat zijn werknemers en/of derden die toegang hebben tot de Persoonsgegevens zicht ertoe hebben gebonden verbonden vertrouwelijkheid in acht te nemen.

5.3 Verwerker zal alle Persoonsgegevens retourneren aan Verwerkingsverantwoordelijke en/of al

deze informatie en eventuele kopieën hiervan vernietigen binnen 10 (tien) werkdagen na ontvangst van het verzoek daartoe van Verwerkingsverantwoordelijke.

6. DUUR

6.1 De Verwerkingsovereenkomst treedt in werking op het moment van ondertekening en is aangegaan voor de duur van de Hoofdovereenkomst.

6.2 Na afloop van de Verwerkingsactiviteiten zal Verwerker, op verzoek van Verwerkingsverantwoordelijke, alle persoonsgegevens wissen of aan Verwerkingsverantwoordelijke terugbezorgen, en bestaande kopieën verwijderen, tenzij opslag van de persoonsgegevens Unierechtelijk of volgens Nederlands recht verplicht is.

7. WIJZIGING

7.1 Indien zich in de toekomst wijzigingen voordoen in de nationale of Europese regelgeving over de bescherming van Persoonsgegevens, zullen Partijen deze Verwerkingsovereenkomst wijzigen voor zover dit nodig is om aan die nieuwe regelgeving te voldoen.

8. OVERDRACHT

8.1 De tussen Verwerker en Verwerkingsverantwoordelijke gesloten Verwerkingsovereenkomst en de daaruit voortvloeiende rechten en verplichtingen kunnen niet aan derden worden overgedragen zonder de schriftelijke toestemming van de andere partij.

9. APPENDICES

9.1 De Appendices van de Verwerkingsovereenkomst maken een integraal onderdeel uit van de Verwerkingsovereenkomst. Bij strijd tussen de Appendices en de Verwerkingsovereenkomst, prevaleert de Verwerkingsovereenkomst.

10. TOEPASSELIJK RECHT

10.1 Op deze Verwerkingsovereenkomst is het Nederlandse recht van toepassing.

10.2 Geschillen tussen partijen, die niet in overleg kunnen worden opgelost, zullen worden voorgelegd aan de daartoe bevoegde Nederlandse rechter van de rechtbank Rotterdam, locatie Rotterdam.

Aldus overeengekomen,

Namens:

Verwerkingsverantwoordelijke	**Verwerker**
	
Bedrijf	Mach3builders B.V.
Naam	W. Onis
Functie	Directeur
Datum	18 juli 2022
Plaats	Barendrecht

VERWERKINGSOVEREENKOMST

APPENDIX 1 – VERWERKING VAN PERSOONSGEGEVENS
(Behorende bij de Verwerkingsovereenkomst gesloten tussen Verwerkingsverantwoordelijke en Verwerker betreffende verwerking van Persoonsgegevens)

Doel verwerking
(Door de Verwerkingsverantwoordelijke zelf in te vullen)

Persoonsgegevens
(Door de Verwerkingsverantwoordelijke zelf aan te geven dmv X te plaatsen, eventueel gegevens FG invullen)

Verwerker zal in het kader van deze Verwerkersovereenkomst, de volgende typen persoonsgegevens verwerken in opdracht van Verwerkingsverantwoordelijke:

	Categorie betrokkenen (artikel 4.1/AVG)
	Werknemers; uitzend- en inleenkrachten; sollicitanten
	Leveranciers; afnemers; Verwerkingsverantwoordelijken
	Cliënt-, patiënt- en inwonergegevens
	Kinderen <16 jaar
	Gewone persoonsgegevens (artikel 4.1/AVG)
	Voornaam; achternaam; meisjesnaam; telefoon; bankrekeningnummer; ip-adres; opleiding; logbestanden betreden gebouw; unieke identificatoren; etc
	Bijzondere persoonsgegevens (artikel 9/AVG)
	Ras of etnische afkomst; politieke opvattingen; religieuze of levensbeschouwelijke overtuigingen; lidmaatschap vakbond; genetische gegevens; biometrische gegevens; gegevens over gezondheid, seksueel gedrag of gerichtheid.
	Strafrechtelijke gegevens (artikel 10/AVG)
	Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten
	Data
	Alle gegevens welke geen persoonsgegevens bevatten die de Verwerkingsverantwoordelijke opslaat en/of verwerkt zoals software, tekst, audio, video
	Functionaris Gegevensbescherming (artikel 37/AVG)
	Verwerkingsverantwoordelijke beschikt over een Functionaris Gegevensbescherming.
	Naam: Contactgegevens

VERWERKINGSOVEREENKOMST

APPENDIX 2 – TECHNISCHE EN ORGANISATORISCHE BEVEILIGINGSMAATREGELEN

(Behorende bij de Verwerkingsovereenkomst gesloten tussen Verwerkingsverantwoordelijke en Verwerker betreffende verwerking van Persoonsgegevens)

Beveiligingsmaatregelen per datum inwerkingtreding Verwerkingsovereenkomst:

Deel van de Verwerker:
Beveiliging qua codering:
- Toegang tot de data is afgeschermd met gebruikersnaam en wachtwoord
- Toepassing van input sanitation tegen XSS
- Toepassing van POST/GET opsplitsing
- Databases zijn UTF-8 encoded om encoding bypasses te voorkomen
- Bij uploads wordt op bestandsnamen sanitation toegepast
- Toepassing van MySQL prepared statements om SQL injections tegen te gaan
- Query's worden opgebouwd met named parameters om SQL injections tegen te gaan
- 3rd party code wordt niet gebruikt tenzij het om een zeer vertrouwde bron gaat
- Mail wordt verzonden middels TLS

Beveiliging organisatorisch:
- Verwerkingsverantwoordelijken hebben geen toegang tot ftp op de servers
- Verwerkingsverantwoordelijken hebben geen toegang tot de databases
- Enkel bevoegde medewerkers hebben toegang tot de data
- Ontwikkelde software wordt uitgebreid getest door meerdere medewerkers
- Waar mogelijk en Verwerkingsverantwoordelijke akkoord gaat wordt https/ssl geïnstalleerd zodat al het websiteverkeer over SSL/HTTPS gaat.

Deel van de Sub-verwerker EGP BV (KvK: 20141659):
Beveiliging:
- Alle servers staan achter een firewall die door ons gemanaged wordt
- Dagelijks worden de servers en de data gebackupped
- Een kopie van de data wordt opgeslagen op een 2e locatie
- Alleen toegang vanuit toegewezen IP-adressen
- De data wordt enkel in Nederlandse datacentra opgeslagen

Opsporen datalekken:
- Alles loggen met syslog
- Continu monitoring op afwijkingen in het tcp/ip verkeer
- Continu monitoring op afwijkingen in het 'gedrag' van servers en gebruikers
- Met regelmaat uitvoeren van penetratie testen.

Certificeringen:
ISO 27001 en NEN 7510

Deel van de Sub-verwerker Shock Media B.V. (KvK: 09107826):
Organisatorisch:
- Uitgebreid informatiebeveiliging- en kwaliteitsbeleid
- Medewerkers zijn gescreend en gebonden aan geheimhouding
- Beleid en procedures op het gebied van toegangsbeheer
- Fysieke beveiliging van kantoren en datacenterlocaties
- Beleid en procedures omtrent de oplevering van servers
- Periodieke security awareness trainingen medewerkers

- Streng beleid omtrent werkplekken, authenticatie en gebruik 2FA
- Beleid en procedures op het gebied van patch- en vulnerability management
- Beleid en procedures omtrent de afhandeling van security- incidenten
- Datacenters bevinden zich op geografisch gescheiden locaties binnen Nederland
- Periodieke security assessments en audits
- Responsible disclosure beleid

Beveiliging:

- Gestandaardiseerde installatie en configuratie servers
- Configuratie en monitoring op basis van security/hardening standaarden
- 24*7 monitoringen en opvolging op afwijkingen
- Uitgebreide logging naar een externe beveiligde omgeving
- Geavanceerde security monitoring op afwijkingen/aanvallen/malware
- Doorlopende scans op kwetsbaarheden op omgevingen
- Toepassing van netwerksegmentatie en beveiliging
- Toegang omgevingen enkel op basis van whitelisting
- Omgevingen worden beveiligd middels firewalls
- Standaard redundantie van Cloud Servers
- Redundante voeding en netwerkverbindingen
- Gebruik NaWas voor DDoS- bescherming
- Toegangsbeveiliging en controle

Back-up en restore

- Dagelijks worden back-ups gemaakt van alle omgevingen.
- Back-ups worden opgeslagen op een geografisch gescheiden datacenterlocatie.
- Back-up retentie (3 volledige en 5 incrementele back-ups) minimaal 21 dagen.
- Uitgebreid Business Continuïty plan en periodieke testen

Certificeringen

ISO 27001; ISO 9001 en NEN 7510

Deel van de Sub-verwerker Savvii B.V. (KvK: 58599541):

Savvii Managed Hosting is ISO 9001 en ISO 27001 gecertificeerd. Zowel het kwaliteitsbeheersysteem als het informatie-veiligheidssysteem voldoet aan de eisen die het International Organization for Standardization (ISO) oplegt. De ISO 9001-norm is in het leven geroepen om te voorzien in een praktisch en goed uitvoerbaar kwaliteitsbeheerssysteem. Het ISO 27001-certificaat waarborgt de bescherming van gevoelige informatie tegen onbevoegde toegang.

Deel van de Sub-verwerker DigitalOcean, LLC

ISO/IEC 27001:2013 - The DigitalOcean Information Security Management System (ISMS) protects assets associated with developing, operating, and maintaining the cloud infrastructure platform.The in-scope products include: Droplets (Virtual Private Servers), Volumes (BlockStorage), and Spaces (Object Storage). The software systems, hardware, people, and processes associated with the in-scope products are globally implemented and operationalized.

Deel van de Sub-verwerker AWS

AWS is verantwoordelijk voor het beveiligen en compliant laten zijn van de hele infrastructuur waarop alle door de klant gekozen diensten beschikbaar zijn. Dit omvat onder andere alle hardware- en software stacks, networking en de fysieke locaties waar de public clouddiensten draaien.