VERWERKERSOVEREENKOMST

Partijen:

1. **Mentix Media h.o.d.n. Webday**, gevestigd te Rijen, hierna: **"Verwerker"**; en
2. **De wederpartij** aan wie Verwerker diensten verleent (de klant), hierna: **"Verwerkingsverantwoordelijke"**.

Overwegende dat:

- Verwerkingsverantwoordelijke gebruik maakt van de diensten van Verwerker (zoals hosting, onderhoud of development);
- Verwerker hierbij persoonsgegevens verwerkt ten behoeve van Verwerkingsverantwoordelijke;
- Partijen hun rechten en plichten omtrent deze verwerking wensen vast te leggen conform de AVG.
- Deze overeenkomst onlosmakelijk verbonden is met de Algemene Voorwaarden van Webday.

Komen het volgende overeen:

Artikel 1 – voorwaarden voor gegevensverwerking

1. Tijdens het verstrekken van diensten aan de Verwerkingsverantwoordelijke, kan de Verwerker namens de Verwerkingsverantwoordelijke persoonsgegevens verwerken volgens de voorwaarden van deze Overeenkomst. De Verwerker stemt ermee in om te voldoen aan de hand van de volgende bepalingen met betrekking tot alle persoonsgegevens die namens de Verwerkingsverantwoordelijke worden verwerkt.
2. De Verwerkingsverantwoordelijke is als enige verantwoordelijk voor de juistheid, kwaliteit en wettigheid van de persoonsgegevens die namens de Verwerkingsverantwoordelijke worden verwerkt en de wijze waarop de Verwerkingsverantwoordelijke persoonsgegevens heeft verkregen.

Artikel 2 – Verwerking van persoonsgegevens

1. Verwerker zal persoonsgegevens uitsluitend verwerken voor de volgende doeleinden: (i) verwerking in overeenstemming met de dienstverlening van Verwerker met betrekking tot het hosten en onderhouden van websites; (ii) verwerking geïnitieerd door geautoriseerd personeel van de Verwerkingsverantwoordelijke bij hun gebruik van de diensten van Verwerker; en (iii) verwerking om te voldoen aan andere redelijke instructies die door de Verwerkingsverantwoordelijke worden verstrekt (bijv. via e-mail of ondersteuningstickets) die in overeenstemming zijn met de voorwaarden van de diensten (individueel en collectief hierna te noemen: het "Doel").

2. In overeenstemming met artikel 28 lid 3, onder a, AVG zal de Verwerker geen persoonsgegevens verwerken anders dan in overeenstemming met de gedocumenteerde instructies van de Verwerkingsverantwoordelijke.
3. De inhoud van de verwerking van persoonsgegevens door Verwerker is gelijk aan het Doel, zoals beschreven in artikel 2.1. De duur van de verwerking, de aard en het doel van de verwerking, de soorten persoonsgegevens en categorieën van betrokkenen die in het kader van deze verwerkersovereenkomst worden verwerkt, worden nader gespecificeerd in bijlage 1 bij deze verwerkersovereenkomst.

Artikel 3 – Vertrouwelijkheid

1. In overeenstemming met artikel 28 lid 3, onder b, AVG moet Verwerker ervoor zorgen dat alle personen die de plicht hebben om namens de Verwerkingsverantwoordelijke persoonsgegevens te verwerken, onderworpen zijn aan vertrouwelijkheidsverplichtingen of professionele of wettelijke geheimhoudingsverplichtingen.

Artikel 4 – Beveiliging van persoonsgegevens

1. Verwerker zal passende technische en organisatorische maatregelen nemen ter bescherming van de veiligheid, vertrouwelijkheid en integriteit van persoonsgegevens, zoals uiteengezet in bijlage 2 (Technische en Organisatorische maatregelen). Verwerker ziet regelmatig toe op de naleving van deze maatregelen en zal zorgen voor een proces voor het regelmatig testen, beoordelen en evalueren van de effectiviteit van dergelijke technische en organisatorische maatregelen om de veiligheid van de verwerking te waarborgen. Verwerker zal de algehele veiligheid van de diensten gedurende de looptijd van de overeenkomst tussen partijen niet wezenlijk verminderen.

Artikel 5 – Sub-verwerking

1. In overeenstemming met artikel 28 lid 4 AVG kan de Verwerker sub-verwerkers inschakelen uitsluitend in overeenstemming met de schriftelijke toestemming van de Verwerkingsverantwoordelijke. Verwerker blijft volledig aansprakelijk jegens de Verwerkingsverantwoordelijke voor het niet-nakomen door elke sub-verwerker van zijn verplichtingen met betrekking tot de verwerking van persoonsgegevens namens de Verwerkingsverantwoordelijke.
2. Verwerkingsverantwoordelijke geeft toestemming om de sub-verwerkers zoals genoemd in bijlage 3 te gebruiken.

Artikel 6 – Rechten betrokkenen

1. In overeenstemming met artikel 12, artikel 28 lid 3, onder e, en artikel 31 AVG zal de Verwerker de Verwerkingsverantwoordelijke onmiddellijk op de hoogte stellen als hij een verzoek ontvangt van een persoon of een andere bevoegde autoriteit conform de AVG met betrekking tot persoonsgegevens die op basis van de AVG worden verwerkt namens de Verwerkingsverantwoordelijke. De Verwerker zal redelijkerwijs meewerken indien gevraagd door de Verwerkingsverantwoordelijke om de Verwerkingsverantwoordelijke in staat te stellen te voldoen aan de uitoefening van rechten door een betrokkene conform de AVG.

Artikel 7 – Datalekken

1. De Verwerker zal de Verwerkingsverantwoordelijke zonder onnodige vertraging en in ieder geval binnen vierentwintig (24) uur op de hoogte stellen, zodra hij kennis heeft genomen van of redelijkerwijs vermoedt dat er sprake is van een inbreuk in verband met persoonsgegevens. De kennisgeving bevat ten minste de informatie zoals gedefinieerd in artikel 33 lid 3, AVG.
2. De melding wordt per e-mail verzonden naar een bekend mailadres van de Opdrachtgever
3. In het geval van een inbreuk in verband met persoonsgegevens zal de Verwerker geen derde partij informeren zonder eerst de voorafgaande schriftelijke toestemming van de Verwerkingsverantwoordelijke te hebben verkregen. De Verwerker zal samenwerken met de Verwerkingsverantwoordelijke en alle redelijke stappen ondernemen die door de Verwerkingsverantwoordelijke worden aangegeven om te helpen bij het onderzoek, de beperking en het herstel van elke inbreuk in verband met persoonsgegevens.

Artikel 8 – Gegevensbeschermingseffectbeoordelingen en voorafgaande raadpleging

1. De Verwerker zal redelijke bijstand verlenen aan de Verwerkingsverantwoordelijke bij alle gegevensbeschermingseffectbeoordelingen die vereist zijn op grond van artikel 35 van de AVG en bij eventuele voorafgaande raadplegingen aan een toezichthoudende autoriteit van de Verwerkingsverantwoordelijke die vereist zijn op grond van artikel 36 van de AVG.

Artikel 9 – Wissen of retourneren van persoonsgegevens

1. In overeenstemming met artikel 28 lid 3, onder g, AVG zal de Verwerker onmiddellijk en in elk geval binnen 30 (dertig) kalenderdagen na: (i) stopzetting van het verwerken van persoonsgegevens door Verwerker conform de onderliggende dienstverlening; of (ii) beëindiging van het gebruik van diensten van Verwerker, naar keuze van Verwerkingsverantwoordelijke, ofwel:
   Een volledige kopie van alle persoonsgegevens aan de Verwerkingsverantwoordelijke retourneren en alle andere kopieën van persoonsgegevens die door de Verwerker of een erkende sub-verwerker zijn verwerkt, veilig wissen, ofwel;
   Veilig alle kopieën van persoonsgegevens wissen die door de Verwerker of een geautoriseerde sub-verwerker zijn verwerkt en in elk geval een schriftelijke verklaring verstrekken aan de Verwerkingsverantwoordelijke dat de Verwerker volledig heeft voldaan aan de vereisten van dit artikel 9.

Artikel 10 – Auditrechten

1. Verwerkingsverantwoordelijke kan ten minste eenmaal per jaar controleren of Verwerker voldoet aan zijn verplichtingen uit hoofde van deze verwerkersovereenkomst, waarvoor hij een derde partij kan gebruiken, op voorwaarde dat de derde partij de audit uitvoert onder de toepassing van een geheimhoudingsverklaring.

2. Verwerker verleent Verwerkingsverantwoordelijke volledige medewerking met betrekking tot een dergelijke audit en verstrekt de Verwerkingsverantwoordelijke op verzoek van de Verwerkingsverantwoordelijke het bewijs dat hij voldoet aan zijn verplichtingen uit hoofde van deze verwerkersovereenkomst.
3. Verwerkingsverantwoordelijke zal Verwerker alle auditrapporten verstrekken die in verband met de audit zijn opgesteld, tenzij dit verboden is door de toepasselijke wetgeving. Auditrapporten worden door de Verwerkingsverantwoordelijke alleen gebruikt om te voldoen aan zijn auditvereisten onder de wetgeving inzake gegevensbescherming en/of om de naleving van deze verwerkersovereenkomst te bevestigen.
4. Verwerker zal commercieel redelijke inspanningen leveren om het niet-naleven van deze verwerkersovereenkomst aan te pakken, op voorwaarde dat als Verwerker nalaat of weigert om dergelijk niet-naleven tijdig aan te pakken binnen minder dan 30 (dertig) dagen na ontvangst van het auditrapport, Verwerkingsverantwoordelijke de niet-conforme diensten kan beëindigen met een schriftelijke kennisgeving van 10 (tien) dagen zonder boete. Verwerker zal Verwerkingsverantwoordelijke alle vooruitbetaalde vergoedingen terugbetalen die de rest van de looptijd van dergelijke diensten dekken na beëindiging zonder een boete voor een dergelijke beëindiging op te leggen aan de Verwerkingsverantwoordelijke.

Artikel 11 – Internationale overdracht van persoonsgegevens van verwerkingsverantwoordelijken

1. De partijen erkennen en komen overeen dat wanneer persoonsgegevens van een betrokkene uit de EER, Zwitserland of het Verenigd Koninkrijk worden verwerkt in een derde land, die rechtstreeks of via verdere doorgifte aan Verwerker worden doorgegeven, hetzij rechtstreeks, hetzij via verdere doorgifte, deze overdracht plaatsvindt onder de voorwaarden die zijn vastgelegd in hoofdstuk V van de AVG.
2. De Verwerker staat niet toe dat een sub-verwerker namens de Verwerkingsverantwoordelijke persoonsgegevens verwerkt in een derde land, dat niet Zwitserland of het Verenigd Koninkrijk of in de EER ligt, en die geen passend beschermingsniveau waarborgt conform privacywetgeving, tenzij vooraf schriftelijk toestemming is gegeven door Verwerkingsverantwoordelijke, via een wijziging van deze verwerkersovereenkomst, in overeenstemming met artikel 5 van deze verwerkersovereenkomst.

Artikel 12 – Algemeen

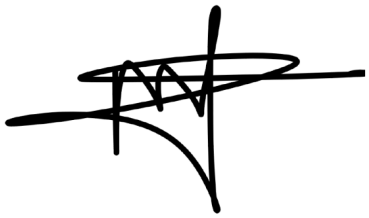
1. Met inachtneming van dit artikel komen de partijen overeen dat deze verwerkersovereenkomst automatisch eindigt bij beëindiging van het gebruik van diensten die door Verwerker worden verstrekt aan de Verwerkingsverantwoordelijke.
2. Elke verplichting die op grond van deze verwerkersovereenkomst aan de Verwerker wordt opgelegd met betrekking tot het verwerken van persoonsgegevens namens de Verwerkingsverantwoordelijke, blijft van kracht na beëindiging of afloop van deze verwerkersovereenkomst.

3. Deze verwerkersovereenkomst wordt beheerst door Nederlands recht.
4. Met betrekking tot de inhoud van deze verwerkersovereenkomst, in geval van afwijkingen tussen de bepalingen van deze verwerkersovereenkomst en andere overeenkomsten tussen de partijen, inclusief maar niet beperkt tot de overeenkomst met betrekking tot de diensten van Verwerker, prevalerende bepalingen van deze verwerkersovereenkomst met betrekking tot de gegevensbeschermingsverplichtingen van de partijen voor persoonsgegevens van een betrokkene.
5. Mocht een bepaling van deze verwerkersovereenkomst ongeldig of niet-afdwingbaar zijn, dan blijven de resterende bepalingen van deze verwerkersovereenkomst geldig en van kracht. De ongeldige of niet-afdwingbare bepaling zal ofwel: (i) indien nodig, worden gewijzigd om de geldigheid en afdwingbaarheid ervan te waarborgen, met behoud van de bedoelingen van de partijen zo goed mogelijk, ofwel, als dit niet mogelijk is, (ii) worden geïnterpreteerd op een manier alsof het ongeldige of niet-afdwingbare deel er nooit in was opgenomen.

Aldus opgesteld te Rijen, d.d. 1 januari 2026.

Mentix Media h.o.d.n. Webday

M. Franken



Deze Verwerkersovereenkomst maakt onlosmakelijk deel uit van de dienstverlening van Webday. Door voortgezet gebruik van de diensten na toezending van deze overeenkomst, verklaart de Verwerkingsverantwoordelijke (Opdrachtgever) zich akkoord met de inhoud hiervan.

BIJLAGE 1: BIJZONDERHEDEN OVER DE VERWERKING VAN PERSOONSGEGEVENS VAN DE VERWERKINGSVERANTWOORDELIJKE

Deze bijlage 1 bevat bepaalde details over de verwerking van persoonsgegevens van de Verwerkingsverantwoordelijke zoals vereist door artikel 28 lid 3 AVG.

Onderwerp en duur van de Verwerking van persoonsgegevens van verwerkingsverantwoordelijke:

- Het onderwerp en de duur van de verwerking van persoonsgegevens namens Verwerkingsverantwoordelijke zijn vastgelegd in deze verwerkersovereenkomst.

De aard en het doel van de verwerking van persoonsgegevens:

- De aard en het doel van de verwerking zijn uiteengezet in artikel 2 van deze verwerkersovereenkomst.

De soorten persoonsgegevens die namens de Verwerkingsverantwoordelijke moeten worden verwerkt:

- NAW-gegevens, contactgegevens, betaalgegevens en inloggegevens van Verwerkingsverantwoordelijke en diens klanten/bezoekers.
- Gegevens die bij het online plaatsen en onderhouden van een website horen
- Technische gegevens zoals IP-adressen en logbestanden die voortvloeien uit hosting en onderhoud.

De categorieën van personen op wie de persoonsgegevens betrekking hebben:

- Persoonsgegevens
- Login gegevens

BIJLAGE 2: TECHNISCHE EN ORGANISATORISCHE MAATREGELEN

1. Organisatorische beveiligingsmaatregelen

1.1. Beveiligingsbeheer

a. Beveiligingsbeleid en -procedures: Verwerker dient een beveiligingsbeleid te documenteren met betrekking tot de verwerking van persoonsgegevens.
b. Rollen en verantwoordelijkheden:
    I. Rollen en verantwoordelijkheden met betrekking tot de verwerking van persoonsgegevens worden duidelijk gedefinieerd en toegewezen in overeenstemming met een beveiligingsbeleid.
    II. Tijdens interne reorganisaties of beëindigingen en verandering van dienstverband is de intrekking van rechten en verantwoordelijkheden in combinatie met overdrachtsprocedures duidelijk gedefinieerd.
c. Toegangscontrole beleid: Specifieke toegangscontrolerechten worden toegewezen aan elke persoon die betrokken is bij de verwerking van persoonsgegevens, volgens het “need-to-know”-principe.
d. Resource/asset management: Verwerker heeft een register van de IT-middelen die worden gebruikt voor de verwerking van persoonsgegevens (hardware, software en netwerk). Een specifieke persoon krijgt de taak om het register bij te houden en bij te werken (bijv. IT-medewerker).
e. Change management: Verwerker zorgt ervoor dat alle wijzigingen in het IT-systeem worden geregistreerd en gemonitord door een specifieke persoon (bijv. IT- of beveiligingsmedewerker). Dit proces wordt regelmatig gemonitord.

1.2. Incidentrespons en bedrijfscontinuïteit

a. Afhandeling van incidenten / inbreuken in verband met persoonsgegevens:
    I. Een incidentresponsplan met gedetailleerde procedures wordt gedefinieerd om een effectieve en ordelijke reactie op incidenten met betrekking tot persoonsgegevens te garanderen.
    II. Verwerker zal zonder onnodige vertraging aan Verwerkingsverantwoordelijke elk beveiligingsincident melden dat heeft geleid tot verlies, misbruik of ongeoorloofde verwerving van persoonsgegevens.
b. Bedrijfscontinuïteit: Verwerker stelt de belangrijkste procedures en controles vast die moeten worden gevolgd om het vereiste niveau van continuïteit en beschikbaarheid van het IT-systeem dat persoonsgegevens verwerkt te waarborgen in het geval van een incident / inbreuk in verband met persoonsgegevens.

1.3. Personeelszaken

a. Vertrouwelijkheid van personeel: Verwerker zorgt ervoor dat alle medewerkers hun verantwoordelijkheden en verplichtingen met betrekking tot de verwerking van persoonsgegevens begrijpen. Rollen en verantwoordelijkheden worden duidelijk gecommuniceerd tijdens het pre-employment en/of introductieproces.
b. Training: Verwerker zorgt ervoor dat alle medewerkers adequaat worden geïnformeerd over de beveiligingscontroles van het IT-systeem die betrekking hebben op hun dagelijkse werk. Medewerkers die betrokken zijn bij de verwerking van

persoonsgegevens worden ook naar behoren geïnformeerd over relevante vereisten inzake gegevensbescherming en wettelijke verplichtingen door middel van regelmatige bewustmakingscampagnes.

2. Technische beveiligingsmaatregelen

2.1. Toegangscontrole en verificatie

a. Er wordt een toegangscontrolesysteem geïmplementeerd dat van toepassing is op alle gebruikers die toegang hebben tot het IT-systeem. Het systeem maakt het mogelijk om gebruikersaccounts aan te maken, goed te keuren, te controleren en te verwijderen.
b. Het gebruik van algemene gebruikersaccounts wordt vermeden. In gevallen waarin dit nodig is, wordt ervoor gezorgd dat alle gebruikers van het gemeenschappelijke account dezelfde rollen en verantwoordelijkheden hebben.
c. Bij het verlenen van toegang of het toewijzen van gebruikersrollen zal het "need-to-know”-principe in acht worden genomen om het aantal gebruikers dat toegang heeft tot persoonsgegevens te beperken tot degenen die deze nodig hebben voor het bereiken van de verwerkingsdoeleinden van de Verwerker.
d. Wanneer verificatiemechanismen zijn gebaseerd op wachtwoorden, vereist processor dat het wachtwoord ten minste acht tekens lang is en voldoet aan zeer sterke parameters voor wachtwoordbeheer, waaronder lengte, tekencomplexiteit en niet-herhaalbaarheid.
e. De verificatiegegevens (zoals gebruikers-ID en wachtwoord) worden nooit onbeschermd via het netwerk verzonden.

2.2. Loggen en monitoring

Logbestanden worden geactiveerd voor elk systeem/applicatie die wordt gebruikt voor de verwerking van persoonsgegevens. Ze omvatten alle soorten toegang tot gegevens (bekijken, wijzigen, verwijderen).

2.3. Beveiliging van gegevens

a. Server-/databasebeveiliging
    I. Database- en toepassingsservers zijn geconfigureerd om te worden uitgevoerd met behulp van een afzonderlijk account, met minimale besturingssysteembevoegdheden om correct te functioneren.
    II. Database- en applicatieservers verwerken alleen de persoonsgegevens die daadwerkelijk nodig zijn om de verwerkingsdoeleinden te bereiken.
b. Beveiliging van werkstations:
    I. Gebruikers kunnen de beveiligingsinstellingen niet deactiveren of omzeilen.
    II. Antivirustoepassingen en detectiehandtekeningen worden regelmatig geconfigureerd.
    III. Gebruikers hebben geen rechten om ongeautoriseerde softwaretoepassingen te installeren of te deactiveren.
    IV. Het systeem heeft sessietime-outs wanneer de gebruiker gedurende een bepaalde periode niet actief is geweest.

V. Kritieke beveiligingsupdates die door de ontwikkelaar van het besturingssysteem zijn uitgebracht, worden regelmatig geïnstalleerd.

2.4. Netwerk/Communicatie beveiliging

a. Wanneer toegang wordt uitgevoerd via internet, wordt de communicatie gecodeerd via cryptografische protocollen.
b. Verkeer van en naar het IT-systeem wordt gemonitord en gecontroleerd via firewalls en inbraakdetectiesystemen.

2.5. Back-ups

a. Back-up- en gegevensherstelprocedures zijn gedefinieerd, gedocumenteerd en duidelijk gekoppeld aan rollen en verantwoordelijkheden.
b. Back-ups krijgen een passend niveau van fysieke en milieubescherming dat in overeenstemming is met de normen die worden toegepast op de oorspronkelijke gegevens.
c. De uitvoering van back-ups wordt gemonitord om de volledigheid te waarborgen.

2.6. Mobiele/draagbare apparaten

a. Beheerprocedures voor mobiele en draagbare apparaten worden gedefinieerd en gedocumenteerd en stellen duidelijke regels vast voor het juiste gebruik ervan.
b. Mobiele apparaten die toegang hebben tot het informatiesysteem zijn vooraf geregistreerd en vooraf geautoriseerd.

2.7. **Beveiliging van de levenscyclus van applicaties**

Tijdens de ontwikkelingslevenscyclus worden ‘best practices’, ‘state-of-the-art’ en goed erkende veilige ontwikkelingspraktijken of -normen gevolgd.

2.8. Verwijdering/verwijdering van gegevens

a. Software-gebaseerde overschrijven zal worden uitgevoerd op media voordat ze worden verwijderd. In gevallen waar dit niet mogelijk is, bij onder meer, maar niet uitsluitend cd’s en dvd’s, zal fysieke vernietiging worden uitgevoerd.
b. Het versnipperen van papier en draagbare media die worden gebruikt om persoonlijke gegevens op te slaan, wordt minimaal jaarlijks uitgevoerd.

2.9. Fysieke beveiliging

De fysieke ruimte van de IT-systeeminfrastructuur is niet toegankelijk voor niet-geautoriseerd personeel. Er moeten passende technische maatregelen, waarbij onder andere, maar niet uitsluitend wordt gedoeld op inbraakdetectiesysteem, met chipkaarten bediend tourniquet, eenmansbeveiligingssysteem en sluitsystemen, of organisatorische maatregelen, waarbij onder andere, maar niet uit wordt gedoeld op een bewaker, getroffen worden om beveiligingszones en hun toegangspunten te beschermen tegen toegang door onbevoegden.

BIJLAGE 3: SUB-VERWERKERS

Verwerker maakt in overeenstemming met artikel 28 lid 4 AVG gebruik van de volgende sub-verwerkers:

Naam	Product/dienst	Uitleg
Hoasted	Webhosting en domeinregistratie	Verwerker maakt gebruik van Hoasted voor het hosten van de website en de registratie van domeinnamen van de Verwerkingsverantwoordelijke.
Vimexx	Webhosting en domeinregistratie	Verwerker maakt gebruik van Vimexx voor het hosten van de website en de registratie van domeinnamen van de Verwerkingsverantwoordelijke.
ManageWP (Orion)	WordPress onderhoud	Verwerker maakt gebruik van ManageWP voor het centraal beheren, updaten en monitoren van de beveiliging van de WordPress-websites.
Moneybird / HostFact	Facturatie en administratie	Verwerker maakt gebruik van Moneybird en hostfact voor het verwerken van administratieve gegevens en het factureren van de geleverde diensten.