ZORION

BIJLAGE BIJ DE VERWERKERSOVEREENKOMST

Technische en organisatorische maatregelen

Bijlage 2 bij de kaderverwerkersovereenkomst van Zorion, met een deel per module.

Documenttype	Bijlage bij de verwerkersovereenkomst
Hoort bij	Kaderverwerkersovereenkomst, versie 3.2, 29 oktober 2026
Van toepassing bij	Elke module, telkens het deel van die module
Versie	3.2
Datum	29 oktober 2026
Uitgegeven door	Zorion, Vakenderveld 7 bus 6, 2500 Lier, België, RPR Antwerpen afdeling Mechelen, ondernemingsnummer 1009.162.363
Contact	Luka Stoop, admin@zorion.be

Bijlage 2. Hoe deze bijlage geldt

Voor een verwerkingsverantwoordelijke gelden het deel Bij elke module en de delen van de modules die op zijn voorblad op ja staan. Verwijzingen naar een artikelnummer verwijzen naar de kaderovereenkomst.

Invoer in AI-hulpmiddelen

De verwerker gebruikt AI-hulpmiddelen bij het opstellen en nakijken van documentatie, configuratie en programmacode.

- De verwerker voert enkel de gegevens in die de opdracht vereist. Wat voor de opdracht niet nodig is, wordt vooraf uit het ingevoerde materiaal verwijderd.
- Inloggegevens, sleutels en andere authenticatiegegevens worden nooit ingevoerd.
- De verwerker gebruikt uitsluitend de zakelijke dienstverlening van de aanbieder, waarvoor contractueel vaststaat dat de ingevoerde gegevens niet gebruikt worden om modellen te trainen. Gratis of persoonlijke versies worden niet gebruikt.
- Stelt de verwerker vast dat er meer ingevoerd werd dan de opdracht vereiste, dan behandelt hij dat als een incident volgens procedure P-01.

Gebruik van de aangeboden hulpmiddelen

Of de medewerkers van de verwerkingsverantwoordelijke de aangeboden hulpmiddelen ook effectief gebruiken, ligt bij de verwerkingsverantwoordelijke. De verwerker kan dat gebruik niet afdwingen.

Stelt de verwerker vast dat een hulpmiddel niet of verkeerd gebruikt wordt, dan meldt hij dat aan de verwerkingsverantwoordelijke. Die melding is geen instructie in de zin van artikel 4 en verplaatst de verantwoordelijkheid niet.

Bijlage 2A. Module A, onlineaanwezigheid

Toegangsbeheer en authenticatie

- Toegang tot de hosting, de website, de DNS en de beheersomgevingen verloopt via persoonlijke, benoemde accounts. Gedeelde accounts worden vermeden.
- Wachtwoorden worden uniek gegenereerd en bewaard in Proton Pass, een kluis met zero-knowledge-versleuteling.
- Meervoudige authenticatie is verplicht gesteld voor alle leden van de organisatie van de verwerker, en wordt geactiveerd op elke beheersomgeving van de verwerkingsverantwoordelijke die dit ondersteunt.
- Toegang wordt ingetrokken zodra de noodzaak ervan vervalt.
- De verwerker bewaart op verzoek van de verwerkingsverantwoordelijke diens inloggegevens. Die gegevens staan uitsluitend in de kluis, worden nooit per e-mail of chatbericht doorgegeven, en worden op verzoek van de verwerkingsverantwoordelijke verwijderd.

Versleuteling

- Al het verkeer naar en van de website verloopt versleuteld via TLS. Het certificaat wordt automatisch afgeleverd en verlengd via Let’s Encrypt.
- Combell beschikt voor de hosting over een certificering volgens ISO 27001 voor informatiebeveiliging en ISO 27701 voor gegevensbescherming. De verwerker steunt daarop en houdt de certificaten en de verwerkersovereenkomst van die partij ter beschikking. De verwerker doet zelf geen uitspraak over de fysieke beveiliging van de datacenters.
- De mailservers zijn geconfigureerd voor versleutelde verbindingen bij verzending en ontvangst.
- Ondersteuningssessies op afstand verlopen via Splashtop, over een verbinding die versleuteld is met TLS en AES-256, en enkel na uitdrukkelijke toestemming per sessie.
- Wachtwoorden van websitegebruikers worden door het platform als onomkeerbare hash opgeslagen.

Beveiliging van de applicatie

- De kern van het platform, het thema en de plug-ins worden opgevolgd via een centraal beheersysteem dat de verwerker zelf host, en worden bijgewerkt zodra beveiligingsupdates beschikbaar zijn.
- Een applicatiefirewall filtert verdacht verkeer en blokkeert herhaalde mislukte inlogpogingen. Bij de gratis uitvoering van die firewall komen nieuwe regels en handtekeningen dertig dagen later beschikbaar dan bij de betalende uitvoering.
- De deelname aan het gedeelde netwerk van de firewallleverancier staat standaard uit. Daardoor worden er geen IP-adressen van bezoekers naar die leverancier verzonden.
- Een periodieke scan controleert de bestanden van de website op gekende malware.
- Componenten die niet langer ondersteund worden, worden vervangen of verwijderd.

Beschikbaarheid en herstel

- De website, de databank en de basismailboxen worden gehost bij de hostingprovider vermeld in de subverwerkersbijlage, in datacenters in België.
- Er wordt dagelijks een back-up genomen van de bestanden en van de volledige databank. De bewaartermijn wordt bepaald door de hostingprovider. De verwerker deelt de op dat ogenblik geldende termijn op eenvoudig verzoek mee.
- Herstel uit een back-up is technisch mogelijk.

Aanvullende maatregelen bij een webshop

Deze maatregelen gelden enkel wanneer de website een webshop bevat.

- De betaling verloopt via een externe betaalpagina van de betaaldienst.
- De verbinding naar de bestel- en betaalpagina's verloopt versleuteld via TLS.
- De beheertoegang tot de bestellingen wordt beperkt tot de personen die de verwerkingsverantwoordelijke aanduidt.
- De koppeling met de betaaldienst wordt ingericht met sleutels die in de kluis bewaard worden en die enkel voor die website gelden.
- Bestel- en klantgegevens worden enkel voor marketing gebruikt op uitdrukkelijke opdracht van de verwerkingsverantwoordelijke; module D is dan van toepassing.

Bezoekersstatistieken

- De verwerker richt de bezoekersstatistieken pas in wanneer er een werkende toestemmingsoplossing draait: ofwel de optie toestemmingsbeheer, ofwel een eigen oplossing van de verwerkingsverantwoordelijke die hij schriftelijk bevestigt.
- De bezoekersstatistieken worden uitsluitend geactiveerd nadat de bezoeker daarvoor geldige toestemming heeft gegeven.
- Het account bij Google staat op naam van de verwerkingsverantwoordelijke, die er de contractpartij van is en de verwerkingsvoorwaarden van Google zelf aanvaardt. De verwerker aanvaardt die voorwaarden enkel met diens schriftelijke opdracht en in diens naam.

Toestemming voor commerciële e-mails

Deze maatregelen gelden enkel wanneer de verwerker op de website de module Toestemming van zijn eigen plug-in inricht.

- Het register staat in de databank van de website zelf, bij de hostingprovider vermeld in de subverwerkersbijlage.
- Het register bevat enkel wat nodig is om de toestemming aan te tonen: de gegevens vermeld in bijlage 1A. Er wordt geen IP-adres opgeslagen.
- Elke wijziging van de toestemmingstekst, van de naam van de verwerkingsverantwoordelijke of van de link naar de privacyverklaring levert een nieuwe tekstversie op. Elke inschrijving blijft verwijzen naar de versie die de betrokkene zag.
- Het vinkvak staat nooit vooraf aangevinkt. Dubbele opt-in staat standaard aan, zodat een inschrijving pas actief wordt na een bevestigingsklik in een mail aan het opgegeven adres. Zij wordt voor een doel enkel uitgezet op schriftelijke instructie van de verwerkingsverantwoordelijke.
- Bevestigen en afmelden gebeurt met een knop op een eigen pagina zonder scripts van het thema, die niet in een cache of een zoekmachine terechtkomt en geen verwijzende pagina doorgeeft. Een afmelding trekt elke open inschrijving van dat adres voor dat doel in.
- Een inschrijving is beveiligd met een eenmalige code en een lokveld, beperkt tot vijf inschrijvingen per adres per uur en honderd bevestigingsmails per uur voor de hele website, en verloopt onder een vergrendeling in de databank per adres en doel.
- Exporteren, manueel intrekken en instellingen wijzigen kan enkel met beheerdersrechten op de website. Elke beheeractie komt in een logboek met tijdstip, gebruiker en handeling; het logboek wordt twee jaar bewaard.
- Een ingetrokken inschrijving wordt gewist 365 dagen na de intrekking, of na de termijn die de verwerkingsverantwoordelijke per doel opgeeft overeenkomstig artikel 10.1. Een onbevestigde inschrijving wordt na dertig dagen gewist.
- Een verzoek tot wissing via de privacyhulpmiddelen van de website trekt een actieve inschrijving in; zij blijft bewaard tot het einde van de bewaartermijn.
- Het register blijft bewaard wanneer de plug-in verwijderd wordt, tenzij een beheerder uitdrukkelijk kiest om het mee te wissen.
- Een afmelding die in een verzendplatform binnenkomt, komt niet vanzelf in het register. Beheert de verwerker het verzendplatform, dan geldt bijlage 2D; anders staat de verwerkingsverantwoordelijke daar zelf voor in.

Logging en opvolging

- De hostingprovider houdt toegangs- en serverlogs bij.
- De applicatiefirewall registreert geblokkeerde en verdachte handelingen.
- Logs worden geraadpleegd bij een melding of bij een vermoeden van een incident. Er is geen doorlopende, geautomatiseerde analyse van logbestanden.

Organisatorische maatregelen

- De vaststellingen van de evaluatie bedoeld in artikel 6.6 worden bijgehouden.
- De lijst van subverwerkers wordt minstens jaarlijks nagekeken.

Beperkingen eigen aan het gekozen pakket

Dit zijn de beperkingen bedoeld in artikel 6.3. Elke rij waarin het afgenomen pakket voorkomt, is op de verwerkingsverantwoordelijke van toepassing.

Pakket	Beperking
Hostingpakket Legacy	Geen actieve bewaking, geen periodieke kwetsbaarheidsrapportage, geen gegarandeerde reactie- of hersteltermijn. Een incident wordt vastgesteld nadat de verwerkingsverantwoordelijke het meldt.
Seed, Grow en Scale, website bij de verwerker	Bewaking van de bereikbaarheid van de website tijdens de bedrijfsuren, in de vorm van een melding wanneer zij onbereikbaar is. Geen bewaking buiten die uren, geen berekening van de beschikbaarheid over de tijd en geen doorlopende analyse van logbestanden.
Seed, Grow en Scale, website binnen Odoo	Geen bewaking van de domeinnaam en de DNS.
Marketing Master	Dezelfde beperkingen als het pakket waarbinnen de website of de domeinnaam geleverd wordt. Levert de verwerker enkel de domeinnaam, dan is er binnen deze module geen bewaking.

Een dienst met permanente bewaking zit niet in deze pakketten en wordt afzonderlijk geoffreerd.

Bijlage 2B. Module B, Microsoft 365

Identiteit en toegang

- Elke gebruiker heeft een persoonlijk account. Gedeelde accounts worden vermeden; waar een gemeenschappelijk adres nodig is, gebeurt dat via een gedeeld postvak zonder eigen aanmelding.
- Meervoudige authenticatie is verplicht voor alle gebruikers. De verwerker dwingt dat af op tenantniveau, zodat het niet per gebruiker kan worden uitgeschakeld.
- De beveiligingsstandaarden van het platform zijn geactiveerd, met verhoogde bescherming voor beheerdersaccounts.
- Rechten worden toegekend volgens het beginsel van minimale toegang. Bij uitdiensttreding wordt het account onmiddellijk geblokkeerd, worden de actieve sessies verbroken en wordt de licentie vrijgegeven volgens procedure P-04.
- De verwerker gebruikt een afzonderlijk, benoemd beheerdersaccount in de omgeving van de verwerkingsverantwoordelijke en bewaart de inloggegevens in de kluis beschreven in bijlage 2A. Hij werkt niet met het account van de verwerkingsverantwoordelijke zelf.

Bescherming van berichten en bestanden

- Versleuteling van gegevens tijdens transport en in rust volgens de standaardmaatregelen van het platform.
- Filtering van schadelijke bijlagen en koppelingen in inkomende berichten, binnen de mogelijkheden van de licentie die bij het pakket hoort.
- Mailauthenticatie ingesteld via SPF, DKIM en DMARC op het domein van de verwerkingsverantwoordelijke.
- Een bewaarbeleid voor verwijderde items en een versiegeschiedenis voor bestanden, binnen wat de licentie toelaat.
- Externe deling van bestanden wordt beperkt tot wat de verwerkingsverantwoordelijke uitdrukkelijk wenst, en anonieme deelkoppelingen zonder vervaldatum staan uit.

Opvolging

- De beveiligingsmeldingen die het platform zelf genereert, worden doorgestuurd naar het beheeradres van de verwerker en beoordeeld tijdens de bedrijfsuren.
- Stelt de verwerker een verdachte aanmelding vast, dan brengt hij de verwerkingsverantwoordelijke daarvan op de hoogte en stelt hij voor om het wachtwoord te vernieuwen en de sessies te verbreken.
- Licentiegebruik wordt elk kwartaal nagekeken op accounts van vertrokken medewerkers.
- Toegangsrechten worden, naast de herziening van artikel 6.6, nagekeken bij elke wijziging in het personeelsbestand die de verwerkingsverantwoordelijke meldt.

Beperkingen eigen aan deze module

Overeenkomstig artikel 6.3 gelden bij elk pakket van deze module de volgende beperkingen:

- Geen apparaatbeheer en geen mobiel apparaatbeheer, en geen onafhankelijke back-up, tenzij de verwerkingsverantwoordelijke die opties afneemt.
- Geen geavanceerde compliance en geen gegevensverliespreventie.
- Migratie vanuit oude systemen valt buiten de module.
- Geen permanente bewaking buiten de bedrijfsuren.
- Geen beveiligingsscans die verder gaan dan wat het platform standaard rapporteert.

Bijlage 2C. Module C, Odoo

Toegang binnen de omgeving

- Gebruikers krijgen rechten op basis van hun rol.
- Meervoudige authenticatie is verplicht voor alle interne gebruikers. De verwerker dwingt haar af op het niveau van de omgeving, zodat zij niet per gebruiker kan worden uitgeschakeld, en past dezelfde regel toe op zijn eigen omgeving.
- De omgeving houdt bij wie welke gegevens heeft aangemaakt of gewijzigd.
- Toegang van de verwerker wordt beperkt tot wat nodig is voor implementatie, ondersteuning en onderhoud, en wordt ingetrokken zodra die noodzaak vervalt.

Het beheerdersaccount van de verwerker

De verwerker werkt binnen de omgeving van de verwerkingsverantwoordelijke met een eigen benoemd account, en niet met het account van de verwerkingsverantwoordelijke. De verwerkingsverantwoordelijke voorziet daarvoor één bijkomende gebruikerslicentie.

Enkel met schriftelijke toestemming van beide partijen delen zij in afwijking daarvan één account. De verwerkingsverantwoordelijke geeft die toestemming met een schriftelijke bevestiging volgens het sjabloon van de verwerker. Die bevestiging mag elektronisch gebeuren, met een elektronische handtekening of met een aanvaarding via een link. De verwerkingsverantwoordelijke aanvaardt dan dat in de logbestanden niet zichtbaar is wie de handeling stelde. De verwerker houdt in dat geval zelf een werkverslag bij van zijn tussenkomsten en legt dat op verzoek voor.

Implementatie en migratie

- Gegevens worden ingelezen op basis van een gecontroleerd invoerbestand, met een validatie voor en na de invoer.
- Bij een migratie beslissen de partijen vooraf welke gegevens overkomen en welke bewust achterblijven.
- Testgegevens worden niet in de productieomgeving achtergelaten.
- Bevat een testomgeving echte persoonsgegevens, dan geldt daar hetzelfde beschermingsniveau als in productie.

Beschikbaarheid en herstel

- De omgeving wordt gehost bij de hostingpartij van het platform. Voor de fysieke beveiliging van de datacenters steunt de verwerker op de maatregelen en verklaringen van die hostingpartij, en houdt hij die documentatie ter beschikking.
- Back-ups worden genomen door de hostingpartij, volgens diens frequentie en bewaartermijn. De verwerker maakt geen afzonderlijke back-up en belooft geen eigen hersteltermijn.
- Herstel uit een back-up wordt aangevraagd bij de hostingpartij. De verwerker begeleidt dat en volgt het op namens de verwerkingsverantwoordelijke, maar de uitvoeringstermijn ligt bij die partij.

Werkwijze bij ondersteuning

- Ondersteuning verloopt via de omgeving zelf, niet via het uitwisselen van gegevensbestanden per e-mail.
- Is een uittreksel nodig om een fout te onderzoeken, dan wordt dat beperkt tot de betrokken gegevens en na afhandeling verwijderd.
- Sessies op afstand verlopen versleuteld en enkel na uitdrukkelijke toestemming per sessie.

Bezoekersstatistieken van de website binnen Odoo

Bij een contract met module D geldt voor de website binnen Odoo als werkende toestemmingsoplossing: ofwel de optie toestemmingsbeheer, ofwel de cookiebalk van Odoo, door de verwerker ingesteld zodat zij diensten van derden blokkeert tot de bezoeker optionele cookies aanvaardt, ofwel een eigen oplossing van de verwerkingsverantwoordelijke die hij schriftelijk bevestigt.

Bijlage 2D. Module D, marketing

Toestemming en afmelding

- Inschrijvingen verlopen via een formulier dat vastlegt wanneer, waarvoor en vanaf welke pagina is ingestemd. De verwerker bewaart die vastlegging zolang de inschrijving loopt en nog twee jaar nadien, tenzij de verwerkingsverantwoordelijke overeenkomstig artikel 10.1 een andere termijn opgeeft. Loopt de inschrijving via de module Toestemming op een website onder module A, dan gelden de maatregelen en de bewaartermijnen van bijlage 2A.
- Elke campagne bevat een werkende afmeldkoppeling die zonder verdere voorwaarden en zonder aanmelding werkt.
- Een afmelding wordt onmiddellijk verwerkt en het adres komt op de blokkeerlijst van het verzendplatform. Het platform weigert de verzending naar een geblokkeerd adres, ook wanneer datzelfde adres later via een nieuwe lijst wordt ingeladen. De verwerker controleert die instelling bij elke import en legt de vaststelling vast.
- Het register van toestemmingen, afmeldingen en blokkeringen berust bij de verwerkingsverantwoordelijke. De bewijslast voor de toestemming blijft bij hem; de verwerker neemt die niet over. De verwerker stelt een sjabloon ter beschikking om dat register ook te voeren voor de kanalen die de verwerkingsverantwoordelijke zelf beheert.
- Voor de inschrijvingen die via het verzendplatform van de verwerker verlopen, richt de verwerker dat platform zo in dat het tijdstip, de herkomst, de tekst waarmee is ingestemd, de afmeldingen en de blokkeringen erin worden vastgelegd en beschikbaar blijven in een gangbaar, gestructureerd en machineleesbaar formaat. Hij bezorgt die export op verzoek van de verwerkingsverantwoordelijke, en bij de beëindiging van de module overeenkomstig artikel 13. Verlopen de campagnes via de marketingmodule van Odoo, dan staan de betrokken gegevens in de Odoo-omgeving.
- Komt een lijst niet uit de systemen van de verwerker, dan kan de verwerker het bewijs van de toestemming niet leveren. Hij vraagt bij de import naar de herkomst en de grondslag van de lijst, legt vast wat de verwerkingsverantwoordelijke daarover verklaart, en importeert niet zonder die verklaring. Het bewijs zelf blijft bij de verwerkingsverantwoordelijke.
- Toestemming voor statistieken en advertentiecookies verloopt via het toestemmingsbeheer op de website. Er worden geen niet-noodzakelijke cookies geplaatst voordat de bezoeker heeft ingestemd.

Beperking van gegevens

- Statistieken worden in geaggregeerde vorm opgevraagd en gerapporteerd.
- Er worden geen bijzondere categorieën van gegevens gebruikt om segmenten samen te stellen.
- Rapporten bevatten geen individuele persoonsgegevens, tenzij de verwerkingsverantwoordelijke daar uitdrukkelijk om vraagt en er een grond voor is.
- Lijsten worden niet gedeeld tussen verschillende verwerkingsverantwoordelijken, en er wordt geen enkel profiel over klanten heen opgebouwd.

Verzending

- Mailauthenticatie via SPF, DKIM en DMARC ingesteld op het domein van de verwerkingsverantwoordelijke.
- Campagnes vertrekken van een afzenderadres op het eigen domein van de verwerkingsverantwoordelijke. Er wordt niet verzonden vanaf een technisch adres van een platform.
- Toegang tot het verzendplatform verloopt via persoonlijke accounts met meervoudige authenticatie.

Bezoekersstatistieken

- Beheert de verwerker de website, onder module A of module C, dan stelt hij de bezoekersstatistieken in, op het account op naam van de verwerkingsverantwoordelijke, zodra er een werkende toestemmingsoplossing draait.
- Beheert de verwerker de website niet, dan plaatst hij de meetcodes enkel met de toegang die de verwerkingsverantwoordelijke hem daarvoor geeft, of laat de verwerkingsverantwoordelijke ze plaatsen door wie zijn website beheert.
- Het account bij Google staat op naam van de verwerkingsverantwoordelijke, die er de contractpartij van is en de verwerkingsvoorwaarden van Google zelf aanvaardt. De verwerker heeft in dat account enkel de toegang die de verwerkingsverantwoordelijke hem geeft, en aanvaardt die voorwaarden enkel met diens schriftelijke opdracht en in diens naam.

Zorion SEO

Deze maatregelen gelden bij Marketing Master en Scale.

- Toegang tot Zorion SEO verloopt via persoonlijke accounts. Voor de medewerkers van de verwerker is tweestapsverificatie verplicht. Gebruikers van de verwerkingsverantwoordelijke zien in het klantportaal enkel wat de verwerker met hen deelt.
- Aan DataForSEO OÜ geeft de verwerker enkel zoekwoorden, het domein van de website en de doelmarkt door, geen gegevens van bezoekers, klanten of contactpersonen.
- Voor de AI-functies gebruikt de verwerker de zakelijke dienstverlening van Anthropic, waarvoor contractueel vaststaat dat de ingevoerde gegevens niet gebruikt worden om modellen te trainen. Op verzoek van de verwerkingsverantwoordelijke zet de verwerker die functies voor hem uit.

Beperkingen eigen aan deze module

Onderdeel	Beperking
Marketing Master, standaardtrap	Enkel opvolging en rapportage van sociale media en websitestatistieken, zonder e-mailcampagnes, abonneelijsten of verzending.
Marketing Master met e-mailmarketing, en Scale	Volledige module, inclusief lijstbeheer en verzending via het verzendplatform uit de subverwerkersbijlage, of bij Scale via de marketingmodule van Odoo.
Alle pakketten	Geen advertentiebeheer, geen aankoop van media, geen contentproductie en geen resultaatgarantie op bereik of conversie.