ZORION

BIJLAGEDOCUMENT BIJ DE VERWERKERSOVEREENKOMST

Module B. Microsoft 365, identiteits- en toegangsbeheer

Bijlagen 1, 2 en 3 bij de kaderverwerkersovereenkomst van Zorion. Dit document geldt enkel wanneer module B op het voorblad van die overeenkomst is aangeduid.

Documenttype	Bijlagedocument bij de verwerkersovereenkomst
Module	B. Microsoft 365, identiteits- en toegangsbeheer
Hoort bij	Kaderverwerkersovereenkomst, versie 3.0, 4 oktober 2026
Van toepassing bij	Anchor, Orbit, Grow en Scale
Versie	3.0
Datum	4 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

Verwijzingen naar een artikelnummer verwijzen naar de kaderovereenkomst.

Bijlage 1B. Beschrijving van de verwerking

Onderwerp, aard en doel

Element	Beschrijving
Onderwerp	Het inrichten en beheren van de Microsoft 365-omgeving van de verwerkingsverantwoordelijke: gebruikers, mailboxen, agenda, documentopslag, basisbeveiliging en licenties.
Aard van de verwerking	Aanmaken en beheren van accounts en rechten, configureren van beveiligingsinstellingen, instellen van bewaarbeleid, opvolgen van aanmeldingen, herstel bij verlies van toegang, en het afsluiten van accounts bij uitdiensttreding.
Doel van de verwerking	Uitsluitend het leveren van de overeengekomen diensten. De verwerker leest geen mailboxen of bestanden, tenzij dat noodzakelijk is voor een gemelde storing en na uitdrukkelijke toestemming per geval.
Duur	Zolang de verwerker de Diensten van deze module levert, verlengd met de termijnen bepaald in artikel 13.
Geautomatiseerde besluitvorming	Geen.

Categorieën van betrokkenen

- Medewerkers, zaakvoerders en andere gebruikers van de verwerkingsverantwoordelijke met een account.
- Personen met wie die gebruikers per e-mail of via gedeelde documenten corresponderen.
- Externe gasten die toegang krijgen tot gedeelde mappen of teams.

Soorten persoonsgegevens

Bron	Gegevens
Accountbeheer	Naam, zakelijk e-mailadres, functie, gebruikersnaam, toegewezen licenties en rechten, gegevens voor meervoudige authenticatie (gsm-nummer, geregistreerd toestel).
Mailboxen	Afzender, ontvanger, onderwerp, tijdstip, inhoud van berichten en bijlagen.
Agenda en contacten	Afspraken, deelnemers, locaties en contactgegevens.
Documentopslag	De inhoud van bestanden in OneDrive en SharePoint, met de metadata over wie wat wanneer heeft gewijzigd of gedeeld.
Aanmeldlogs	Tijdstip, IP-adres, locatie, apparaat en resultaat van elke aanmeldpoging.
Beveiligingsmeldingen	Gegevens over geblokkeerde berichten, verdachte aanmeldingen en gedetecteerde bedreigingen.
Bewaarde en verwijderde items	Kopieën die het platform zelf bewaart in de prullenbak, in de bewaarperiode van verwijderde items en in de versiegeschiedenis van bestanden.
Apparaatbeheer, indien afgenomen	Type, besturingssysteem en versie, serienummer of toestel-id, inschrijvingsstatus, toegepaste beleidsregels en naleving ervan. De inhoud van persoonlijke bestanden op het toestel wordt niet verwerkt.

Bron	Gegevens
Onafhankelijke back-up, indien afgenomen	Een kopie van de mailboxen en de documenten buiten het platform, met dezelfde gegevens als hierboven.

Back-ups

Microsoft 365 bevat geen onafhankelijke back-up. Een onafhankelijke back-up is enkel beschikbaar als optie. Zonder die optie blijft herstel beperkt tot de prullenbak, de bewaarperiode, de versiegeschiedenis en het bewaarbeleid van het platform zelf; wordt de omgeving zelf onbeschikbaar, of wordt een gegeven gewist na het verstrijken van de bewaarperiode, dan kan de verwerker dat niet herstellen.

Bijzondere categorieën van persoonsgegevens

De dienstverlening is niet gericht op bijzondere categorieën van persoonsgegevens. De inhoud van mailboxen en documentopslag ligt echter volledig bij de verwerkingsverantwoordelijke en kan zulke gegevens bevatten.

De verwerkingsverantwoordelijke bepaalt wat zijn medewerkers in de omgeving plaatsen en wie waartoe toegang heeft. De verwerker richt op verzoek een afgeschermde map of site met beperkte rechten in, maar kan niet controleren wat er nadien in geplaatst wordt.

Bijlage 2B. Technische en organisatorische maatregelen

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. Zonder apparaatbeheer kan een verloren of gestolen toestel niet op afstand gewist worden.
- 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.

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 3B. Subverwerkers

Subverwerkers die de verwerker inschakelt

Subverwerker	Dienst en gegevens	Locatie van de verwerking	Doorgifte naar een derde land en mechanisme
Microsoft Ireland Operations Ltd.	Platform: alle gegevens bijlage 1B	Europese Unie, beperkte uitzonderingen	DPF, Microsoft Corporation; subsidiair standaardcontractbepalingen
Combell NV	Licentiebeheer: beheerrechten op de tenant, gegevens bijlage 1B	Europese Economische Ruimte	Geen

Afhankelijk van de afgenomen opties

De volgende partijen worden enkel ingeschakeld wanneer de verwerkingsverantwoordelijke de betrokken optie afneemt. Zij zijn hierbij vooraf aangekondigd, zodat er bij ingebruikname geen bijkomende kennisgeving nodig is.

Subverwerker	Dienst en gegevens	Locatie van de verwerking	Doorgifte naar een derde land en mechanisme
Microsoft Ireland Operations Ltd.	Optie apparaatbeheer: toestelgegevens, beleidsregels	Zoals hierboven	Zoals hierboven
Combell NV	Optie back-up: kopie mailboxen, documenten	Europese Economische Ruimte	Geen
Splashtop B.V.	Optie antivirus: toestelgegevens, dreigingsmeldingen	Europese Unie (Duitsland), Verenigde Staten	Standaardcontractbepalingen

Verdere schakels in de keten

Microsoft schakelt zelf subverwerkers in en publiceert daarvan een lijst op zijn Service Trust Portal. Wijzigingen in die lijst meldt de verwerker door volgens artikel 7.3 van de kaderverwerkersovereenkomst.