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 2.3
Van toepassing bij	Anchor, Orbit, Grow en Scale
Versie	2.3
Datum	16 augustus 2026
Uitgegeven door	Zorion, Vakenderveld 7.6, 2500 Lier, België, RPR Antwerpen afdeling Mechelen, ondernemingsnummer 1009.162.363
Contact	Luka Stoop, admin@zorion.be

DIT DOCUMENT STAAT NIET OP ZICHZELF

De artikelen van de kaderovereenkomst gelden onverkort. Deze bijlagen beschrijven wat specifiek is voor module B: welke gegevens worden verwerkt, welke maatregelen gelden en welke subverwerkers worden ingeschakeld.

Verwijzingen naar een artikelnummer verwijzen naar de kaderovereenkomst.

Bijlage 1B. Beschrijving van de verwerking

Module B. Microsoft 365, identiteits- en toegangsbeheer.

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	De duur van de hoofdovereenkomst voor deze module, verlengd met de termijnen bepaald in artikel 13.
Geautomatiseerde besluitvorming	Geen. Beveiligingsmeldingen van het platform leiden tot een menselijke beoordeling, niet tot een automatisch besluit met rechtsgevolgen.

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, en de gegevens die nodig zijn voor meervoudige authenticatie, zoals een gsm-nummer of een 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.

De beheerde wachtwoordopslag staat niet in deze tabel. Dat geldt al vanaf module A en is daar beschreven, ook wanneer de verwerkingsverantwoordelijke geen Microsoft 365 afneemt.

Wat er wel en niet met back-ups gebeurt

Microsoft 365 bevat geen onafhankelijke back-up. Wat het platform wel biedt, is een reeks herstelmogelijkheden binnen het platform zelf. Dat is iets anders, en de verwerker benoemt dat verschil uitdrukkelijk omdat het bij een incident bepalend is.

Wat er wel is	Wat dat betekent
Prullenbak en bewaarperiode	Een verwijderde mail of een verwijderd bestand blijft gedurende de door het platform ingestelde periode herstelbaar. Daarna is het weg.
Versiegeschiedenis	Van een bestand in OneDrive of SharePoint kunnen eerdere versies teruggezet worden.
Bewaarbeleid	De verwerker kan een bewaarbeleid instellen dat items langer bijhoudt dan de standaardperiode, binnen wat de afgenomen licentie toelaat.
Wat er niet is	Er is geen kopie buiten het platform. Wordt de omgeving zelf onbeschikbaar, of wordt een gegeven gewist na het verstrijken van de bewaarperiode, dan kan de verwerker dat niet herstellen. Een onafhankelijke back-up is een afzonderlijke betalende dienst en zit niet in de maandprijs.

EEN BESLISSING DIE DE VERWERKINGSVERANTWOORDELIJKE ZELF MOET NEMEN

Wie een onafhankelijke back-up van mailboxen en documenten wil, moet daarvoor een afzonderlijke dienst afnemen. De verwerker offreert die op verzoek en vermeldt dan de leverancier, de bewaartermijn en de kostprijs.

Neemt de verwerkingsverantwoordelijke die niet af, dan aanvaardt hij dat het herstel beperkt is tot wat het platform zelf aanbiedt. Dat is een verdedigbare keuze voor veel ondernemingen, maar het moet een bewuste keuze zijn.

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 in de praktijk gevoelige gegevens bevatten, bijvoorbeeld in personeelsdossiers, medische attesten of arbeidsongeschiktheidsdossiers.

AANDACHTSPUNT BIJ DE INRICHTING

De verwerkingsverantwoordelijke bepaalt wat zijn medewerkers in de omgeving plaatsen en wie waartoe toegang heeft.

Wie gevoelige dossiers bewaart, houdt die in een afgeschermde map of site met beperkte rechten, niet in een algemeen gedeelde map. De verwerker richt zo'n afgeschermde ruimte op verzoek in, maar kan niet controleren wat er nadien in geplaatst wordt.

Bijlage 2B. Technische en organisatorische maatregelen

Module B. Microsoft 365, identiteits- en toegangsbeheer.

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, en in elk geval voor accounts met beheerdersrechten. De verwerker stelt dat af op tenantniveau in, zodat het niet per gebruiker kan worden uitgeschakeld, en past dezelfde regel toe op zijn eigen omgeving. De werkwijze staat in procedure P-04.
- 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 de stappen in procedure P-04. Die procedure legt ook vast wat er met de mailbox en de persoonlijke bestanden van de vertrekkende medewerker gebeurt, en wie daarover beslist.
- 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, zodat in de logs zichtbaar blijft wie wat heeft gedaan.

Bescherming van berichten en bestanden

De onderstaande maatregelen zijn de instellingen die de verwerker aanbrengt. De werkwijze om ze aan te brengen, te controleren en te herstellen wanneer iemand ze wijzigt, staat in procedure P-04. Die procedure wordt op verzoek voorgelegd.

- 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, zodat misbruik van dat domein beperkt wordt.
- Een bewaarbeleid voor verwijderde items en een versiegeschiedenis voor bestanden, binnen wat de licentie toelaat. Zoals in bijlage 1B beschreven, is dat geen onafhankelijke back-up.
- 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. Er is geen permanente bewaking en geen dienst die buiten de bedrijfsuren opvolgt. De verwerker zegt dat uitdrukkelijk, omdat een belofte van doorlopende opvolging zonder wachtdienst niet waargemaakt kan worden.
- 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 bij het kwartaaloverleg nagekeken, zodat er geen accounts van vertrokken medewerkers blijven bestaan.
- Toegangsrechten worden minstens jaarlijks nagekeken, en bij elke wijziging in het personeelsbestand die de verwerkingsverantwoordelijke meldt.

Beperkingen eigen aan het gekozen pakket

Overeenkomstig artikel 6.3. Enkel de regel van het afgenomen pakket is van toepassing.

Pakket	Beperking
Anchor en Grow	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.
Orbit en Scale	Dezelfde beperkingen als Anchor en Grow. Het verschil met die pakketten zit in de marketingmodule, niet in de Microsoft 365-inrichting.
Alle pakketten	Geen permanente bewaking buiten de bedrijfsuren. Geen beveiligingsscans die verder gaan dan wat het platform standaard rapporteert.

WAT APPARAATBEHEER WEL ZOU TOEVOEGEN

Zonder apparaatbeheer kan de verwerker een verloren of gestolen toestel niet op afstand wissen. De bescherming stopt bij het account, niet bij het toestel: het account kan geblokkeerd worden, de bestanden die al lokaal op het toestel stonden niet.

Wie dat risico niet wil dragen, heeft apparaatbeheer nodig. Dat wordt afzonderlijk geoffreerd, met een licentiekost per toestel.

DE VERWERKER LEVERT DE HULPMIDDELEN, DE VERWERKINGSVERANTWOORDELIJKE BEPAALT HET GEBRUIK

De maatregelen hierboven beschrijven wat de verwerker inricht en aanzet. 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

Module B. Microsoft 365, identiteits- en toegangsbeheer. Deze lijst wordt aangepast volgens de procedure van artikel 7.

Subverwerkers die de verwerker inschakelt

Subverwerker	Dienst en gegevens	Locatie van de verwerking	Doorgifte naar een derde land en mechanisme
Microsoft Ireland Operations Ltd.	Levering van het platform: identiteitsbeheer, mailboxen, agenda, documentopslag, filtering en logging. Verwerkt alle gegevens uit bijlage 1B. Dit is de contracterende entiteit voor zakelijke klanten binnen de Europese Economische Ruimte. De verwerker neemt de licenties af en rekent ze aan kostprijs door, waardoor deze partij een subverwerker van de verwerker is.	Europese Unie, binnen de EU Data Boundary. Microsoft documenteert zelf beperkte uitzonderingen voor ondersteuning, voor onderzoek naar beveiliging en voor wettelijke verplichtingen.	Beperkt. De doorgifte gaat naar Microsoft Corporation, gecertificeerd onder het EU-US Data Privacy Framework, en subsidiair op basis van de standaardcontractbepalingen
Odoo S.A.	Registratie en opvolging van meldingen en vragen van de verwerkingsverantwoordelijke en zijn medewerkers, binnen de bedrijfsomgeving van de verwerker. Verwerkt de contactgegevens van de melder en de inhoud van de melding.	Europese Unie, voor de Europese regio via infrastructuur in België	Opslag en verwerking in de Europese regio: geen. Ondersteuning door personeel buiten de EER: standaardcontractbepalingen uit de regeling van de leverancier.
Atlassian Pty Ltd	Interne planning en opvolging van het werk van de verwerker: taken, projecten en terugkerende controles. Verwerkt de contactgegevens van de betrokken medewerkers van de verwerkingsverantwoordelijke en de omschrijving van het werk. De meldingen zelf worden geregistreerd in de omgeving van Odoo; deze omgeving dient voor de opvolging van het werk dat eruit voortvloeit.	Europese Unie en Verenigde Staten	Ja, naar de VS. Standaardcontractbepalingen.
Microsoft Ireland Operations Ltd.	E-mail en documentopslag van de verwerker zelf, gebruikt bij het behandelen van uw vragen. Verwerkt de correspondentie en de contactgegevens die daarbij worden uitgewisseld.	Europese Unie, binnen de EU Data Boundary. Beperkte uitzonderingen voor ondersteuning en voor onderzoek naar beveiliging.	Beperkt. Naar Microsoft Corporation, gecertificeerd onder het EU-US Data Privacy Framework, en subsidiair de standaardcontractbepalingen.

Subverwerker	Dienst en gegevens	Locatie van de verwerking	Doorgifte naar een derde land en mechanisme
Splashtop B.V.	Ondersteuning op afstand. Kan de gegevens verwerken die tijdens een sessie op het scherm zichtbaar zijn, uitsluitend na uitdrukkelijke toestemming per sessie. De verbinding verloopt versleuteld via TLS met AES-256. De contracterende entiteit voor zakelijke klanten binnen de Europese Unie is Splashtop B.V. te Amsterdam.	Europese Unie, met infrastructuur in Duitsland. Ondersteunende systemen in de Verenigde Staten.	Ja, naar de VS. Standaardcontractbepalingen.
Proton AG	Wachtwoordbeheer voor het team van de verwerkingsverantwoordelijke en voor de inloggegevens die de verwerker namens hem bewaart. Verwerkt accountgegevens en versleutelde inloggegevens. De aanbieder heeft zelf geen toegang tot de inhoud van de kluis.	Zwitserland	Ja, naar Zwitserland. Gedekt door het adequaatheidsbesluit voor Zwitserland; geen bijkomend mechanisme vereist.

De vijf partijen onderaan gelden bij elke module en staan daarom in alle vier de bijlagen 3. Wordt module B toegevoegd bij een klant die al module A had, dan komen zij er geen tweede keer bij: het zijn dezelfde subverwerkers voor dezelfde dienst.

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 van dertig dagen nodig is. Neemt hij de optie niet af, dan verwerken zij geen gegevens.

Partij	Wanneer van toepassing	Locatie en doorgifte
Microsoft Ireland Operations Ltd.	Bij de optie apparaatbeheer. Verwerkt dan bijkomend toestelgegevens, de inschrijvingsstatus van het toestel en de toegepaste beleidsregels.	Zoals hierboven
Aanbieder van de onafhankelijke back-up	Bij de optie onafhankelijke back-up van Microsoft 365. Verwerkt een kopie van de mailboxen en de documenten buiten het platform. De concrete partij wordt bij de inrichting vastgelegd en vooraf meegedeeld overeenkomstig artikel 7.3.	Wordt bij de inrichting vastgelegd; de verwerker kiest een partij met opslag binnen de Europese Economische Ruimte
Splashtop B.V.	Bij de optie eindpuntbeveiliging op de toestellen van de verwerkingsverantwoordelijke. Verwerkt toestelgegevens en meldingen over gedetecteerde bedreigingen.	Europese Unie, met ondersteunende systemen in de Verenigde Staten op basis van de standaardcontractbepalingen

Verdere schakels in de keten

Microsoft schakelt zelf subverwerkers in en publiceert daarvan een lijst op zijn Service Trust Portal, met een aankondigingstermijn voor wijzigingen. De verwerker vraagt die lijst minstens jaarlijks op, houdt hem ter beschikking overeenkomstig artikel 7.7, en meldt wijzigingen die hem worden aangekondigd door aan de verwerkingsverantwoordelijke overeenkomstig artikel 7.3.

Microsoft contracteert uitsluitend op zijn eigen voorwaarden. De verwerker heeft die voorwaarden en het bijhorende gegevensbeschermingsaddendum beoordeeld en bewaart die beoordeling, overeenkomstig artikel 7.6. Dat een leverancier niet onderhandelt, ontslaat de verwerker niet van zijn aansprakelijkheid onder artikel 7.5.

> **WAAROM HIER GEEN BELOFTE STAAT DAT ALLES IN EUROPA BLIJFT**
>
> Microsoft verklaart dat klantgegevens van Microsoft 365 binnen de Europese datagrens worden opgeslagen en verwerkt, en documenteert tegelijk uitzonderingen voor onder meer ondersteuning en beveiligingsonderzoek.
>
> De verwerker neemt die nuance over in plaats van een absolute belofte te doen die hij niet kan controleren. Wie een strikte garantie op Europese verwerking nodig heeft, heeft een andere leverancier of een ander licentiemodel nodig, en dat is een gesprek voordat de inrichting begint.