



VAN OOSTEN ADVIES B.V.

Verwerkersovereenkomst

Op grond van artikel 28 van de Algemene verordening gegevensbescherming (AVG), met bijlagen over rollen, verwerkingen, beveiligingsmaatregelen en subverwerkers

Document	Gegevens
Versie	Versie 1.1 (2026)
Documentcode	VOA-VWO-1.1-2026
Status	Geldig voor overeenkomsten die vanaf 1 november 2026 worden gesloten; voor lopende overeenkomsten volgens artikel 17 van de Algemene Voorwaarden; vaste template, aangegaan door ondertekening van het Opdrachtformulier of de opdrachtbevestiging
Datum	4 oktober 2026
Eigenaar	Van Oosten Advies B.V., KvK 42077708, btw NL869603504B01
Adres	Wilgestraat 40, 4431 CH 's-Gravenpolder, Nederland

Verwerkersovereenkomst

Partijen en totstandkoming

Deze Verwerkersovereenkomst wordt gesloten tussen de onderneming die in het Opdrachtformulier of de opdrachtbevestiging als opdrachtgever is vermeld (hierna: **Verwerkingsverantwoordelijke**) en **Van Oosten Advies B.V.**, gevestigd aan de Wilgestraat 40, 4431 CH 's-Gravenpolder, KvK 42077708 (hierna: **Verwerker**), samen: **Partijen**. Zij komt tot stand door ondertekening van het Opdrachtformulier of door Schriftelijke aanvaarding van een opdrachtbevestiging waarin deze Verwerkersovereenkomst van toepassing is verklaard.

Overwegingen

- a) Partijen hebben een of meer overeenkomsten gesloten voor IT-beheer, consultancy, softwareontwikkeling en/of de levering van licenties, hierna: de **Hoofdovereenkomst**.
- b) Bij de uitvoering van de Hoofdovereenkomst verwerkt Verwerker persoonsgegevens ten behoeve van Verwerkingsverantwoordelijke.
- c) Partijen leggen hun afspraken daarover vast overeenkomstig artikel 28 lid 3 van de Algemene verordening gegevensbescherming (AVG), en voor Belgische Verwerkingsverantwoordelijken mede overeenkomstig de Belgische wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

Artikel 1. Definities

- 1.1** Begrippen als persoonsgegevens, verwerking, verwerkingsverantwoordelijke, verwerker, betrokkene, inbreuk in verband met persoonsgegevens en toezichthoudende autoriteit hebben de betekenis die de AVG daaraan geeft.
- 1.2** **Subverwerker:** een derde die door Verwerker wordt ingeschakeld om ten behoeve van Verwerkingsverantwoordelijke persoonsgegevens te verwerken.
- 1.3** **Bijlagen:** Bijlage 1 (Rollenmatrix), Bijlage 2 (Overzicht van verwerkingen), Bijlage 3 (Beveiligingsmaatregelen) en Bijlage 4 (Subverwerkers en doorgiften), die deel uitmaken van deze Verwerkersovereenkomst.

Artikel 2. Onderwerp en rolverdeling

- 2.1** Verwerker verwerkt de in Bijlage 2 omschreven persoonsgegevens uitsluitend ten behoeve van Verwerkingsverantwoordelijke en voor de uitvoering van de Hoofdovereenkomst. Verwerkingsverantwoordelijke bepaalt het doel en de middelen van die verwerking.
- 2.2** De rol van Verwerker wordt per verwerking bepaald door de aard en het doel van die verwerking, niet door het systeem waarin zij plaatsvindt. Bijlage 1 bevat de rollenmatrix. Kort samengevat: Verwerker is verwerker voor alles wat hij namens

Verwerkingsverantwoordelijke in of met diens omgeving en gegevens doet (waaronder de inhoud van meldingen, bijlagen, monitoring- en back-upgegevens); Verwerker is zelfstandig verwerkingsverantwoordelijke voor zijn eigen contract-, facturatie- en relatiebeheer, voor de metagegevens van meldingen die hij voor zijn eigen administratie en dienstverlening nodig heeft, voor de beveiligingslogboeken van zijn eigen systemen en voor de gegevens die hij als Microsoft-partner op grond van de Microsoft-partnervoorwaarden moet registreren. Op de eigen verwerkingen is de privacyverklaring van Verwerker van toepassing (www.van-oosten.nl/privacy).

- 2.3** Voor clouddiensten van Microsoft die Verwerkingsverantwoordelijke rechtstreeks van Microsoft afneemt (al dan niet via Verwerker als wederverkoper), is Microsoft de verwerker van Verwerkingsverantwoordelijke op grond van de Microsoft Customer Agreement en het Microsoft Products and Services Data Protection Addendum, die Verwerkingsverantwoordelijke zelf aanvaardt. Verwerker is voor die diensten verwerker voor zover hij de omgeving beheert en daarbij toegang heeft tot persoonsgegevens.
- 2.4** Als Verwerkingsverantwoordelijke zelf verwerker is voor een derde (bijvoorbeeld een administratiekantoor voor zijn klanten), meldt hij dat aan Verwerker; Verwerker is dan subverwerker en Partijen stemmen de instructies en meldtermijnen af op de verplichtingen van Verwerkingsverantwoordelijke jegens die derde.
- 2.5** Deze Verwerkersovereenkomst gaat bij strijd voor op de Hoofdovereenkomst en de Algemene Voorwaarden, uitsluitend voor zover het de verwerking van persoonsgegevens betreft.

Artikel 3. Instructies en verplichtingen van Verwerker

- 3.1** Verwerker verwerkt persoonsgegevens uitsluitend op basis van schriftelijke instructies van Verwerkingsverantwoordelijke. De Hoofdovereenkomst, deze Verwerkersovereenkomst en de via de supportkanalen door een bevoegde contactpersoon gegeven opdrachten gelden als instructies. Verwerker informeert Verwerkingsverantwoordelijke onmiddellijk als een instructie naar zijn oordeel in strijd is met de AVG of andere toepasselijke gegevensbeschermingswetgeving. Verwerker voert die instructie niet uit zolang die strijdigheid voortduurt; hervatting vindt plaats op basis van een rechtmatige, gedocumenteerde aangepaste instructie of van een toepasselijke wettelijke verplichting. Als Unie- of lidstatelijk recht Verwerker tot een verwerking verplicht, informeert Verwerker Verwerkingsverantwoordelijke daarover vooraf, tenzij dat recht die informatie om gewichtige redenen van algemeen belang verbiedt.
- 3.2** Verwerker verwerkt geen persoonsgegevens voor eigen doeleinden, met uitzondering van de in Bijlage 1 als eigen verwerking aangemerkte verwerkingen. Het gebruik van geaggregeerde, niet tot personen herleidbare gegevens voor het verbeteren van de dienstverlening is alleen toegestaan als de anonimisering zelf een gedocumenteerde instructie van Verwerkingsverantwoordelijke heeft en onomkeerbaar is; gepseudonimiseerde gegevens blijven persoonsgegevens.
- 3.3** Verwerker verwerkt persoonsgegevens uitsluitend binnen de Europese Economische Ruimte (EER) en in landen met een adequaatheidsbesluit van de Europese Commissie, behalve voor zover in Bijlage 4 per ontvanger een doorgifte naar een derde land is vermeld met de daarvoor geldende waarborg. Bijlage 4 vermeldt per

ontvanger de rechtspersoon, de verwerkingslocatie, de eventuele supporttoegang vanuit een derde land en de doorgiftegrond (adequaateheidsbesluit, waaronder het EU-VS Data Privacy Framework voor de op de DPF-lijst vermelde organisatie, of de standaardcontractbepalingen van de Europese Commissie met de toepasselijke module en aanvullende maatregelen). Als een waarborg vervalt (bijvoorbeeld doordat een certificering of een adequaatheidsbesluit komt te vervallen), stapt Verwerker binnen dertig (30) dagen over op een andere geldige waarborg of schort hij de betreffende doorgifte op, en informeert hij Verwerkingsverantwoordelijke daarover. Verwerker informeert Verwerkingsverantwoordelijke vooraf over iedere nieuwe doorgifte via de procedure van artikel 7.

- 3.4** Verwerker zorgt ervoor dat de personen die onder zijn gezag persoonsgegevens verwerken, tot geheimhouding zijn verplicht en toegang hebben tot niet meer persoonsgegevens dan voor hun taak nodig is.
- 3.5** Verwerker verleent Verwerkingsverantwoordelijke, rekening houdend met de aard van de verwerking, bijstand bij het nakomen van diens verplichtingen inzake de rechten van betrokkenen (artikelen 12 tot en met 22 AVG), beveiliging, meldingen van inbreuken, gegevensbeschermingseffectbeoordelingen en voorafgaande raadpleging (artikelen 32 tot en met 36 AVG). Verzoeken van betrokkenen die Verwerker rechtstreeks ontvangt, stuurt hij binnen twee (2) Werkdagen door aan Verwerkingsverantwoordelijke zonder ze zelf inhoudelijk te beantwoorden.
- 3.6** Bijstand die wettelijk noodzakelijk is voor het nakomen van de AVG door Verwerkingsverantwoordelijke (waaronder de informatie en medewerking bij een inbreuk, bij een verzoek van een betrokkene en bij een verzoek van een toezichthoudende autoriteit) verleent Verwerker tijdig en zonder die afhankelijk te maken van betaling. Voor bijstand die in omvang verder gaat dan wat in de Hoofdovereenkomst is inbegrepen, spreekt Verwerker vooraf een redelijke vergoeding tegen het overeengekomen uurtarief af; bijstand die nodig is door een tekortkoming van Verwerker is kosteloos.
- 3.7** Verwerker houdt een register bij van de verwerkingsactiviteiten die hij ten behoeve van Verwerkingsverantwoordelijke verricht, overeenkomstig artikel 30 lid 2 AVG.

Artikel 4. Verplichtingen van Verwerkingsverantwoordelijke

- 4.1** Verwerkingsverantwoordelijke staat ervoor in dat de verwerking van de persoonsgegevens rechtmatig is, dat hij bevoegd is de persoonsgegevens aan Verwerker te verstrekken, dat de betrokkenen waar nodig zijn geïnformeerd en dat de instructies aan Verwerker in overeenstemming zijn met de toepasselijke wetgeving.
- 4.2** Verwerkingsverantwoordelijke vult in het Opdrachtformulier of de opdrachtbevestiging de klantspecifieke onderdelen van Bijlage 2 in (doeleinden, categorieën betrokkenen en gegevens, bewaartermijnen) en geeft daarbij aan of via de beheerde omgeving structureel bijzondere categorieën van persoonsgegevens (artikel 9 AVG), strafrechtelijke gegevens (artikel 10 AVG) of nationale identificatienummers worden verwerkt. Ook zonder die melding gelden voor dergelijke gegevens de minimale instructies van Bijlage 2, onderdeel C.
- 4.3** Verwerkingsverantwoordelijke is verantwoordelijk voor het beveiligingsbeleid binnen zijn eigen organisatie, voor het gedrag van zijn gebruikers en voor

beveiligingsmaatregelen die hij, na schriftelijk advies van Verwerker met vermelding van de risico's, niet heeft laten toepassen.

Artikel 5. Beveiliging

- 5.1 Verwerker treft passende technische en organisatorische maatregelen om de persoonsgegevens te beveiligen tegen vernietiging, verlies, wijziging, ongeoorloofde verstrekking of toegang, rekening houdend met de stand van de techniek, de uitvoeringskosten, de aard, omvang, context en doeleinden van de verwerking en de risico's voor betrokkenen (artikel 32 AVG). De maatregelen zijn beschreven in Bijlage 3.
- 5.2 Verwerker mag de maatregelen van Bijlage 3 aanpassen aan technische ontwikkelingen, mits het beveiligingsniveau niet daalt. Op verzoek verstrekt Verwerker een actuele beschrijving.
- 5.3 Verwerker garandeert niet dat de beveiliging onder alle omstandigheden doeltreffend is, maar staat in voor de uitvoering van de in Bijlage 3 en de Hoofdovereenkomst concreet omschreven maatregelen.

Artikel 6. Inbreuken in verband met persoonsgegevens

- 6.1 Verwerker informeert Verwerkingsverantwoordelijke zonder onredelijke vertraging, en uiterlijk binnen vierentwintig (24) uur nadat Verwerker daarvan kennis heeft gekregen, over een inbreuk in verband met persoonsgegevens die de door Verwerker verwerkte persoonsgegevens raakt. De melding is gefaseerd: een eerste melding met de dan bekende feiten zodra die beschikbaar zijn, gevolgd door aanvullingen zodra meer bekend is. De melding bevat, voor zover beschikbaar: (a) de aard van de inbreuk; (b) de categorieën en het geschatte aantal betrokkenen en gegevens; (c) de waarschijnlijke gevolgen; (d) de getroffen en voorgestelde maatregelen; (e) de contactpersoon bij Verwerker.
- 6.2 De melding gaat naar de in het Opdrachtformulier aangewezen contactpersoon voor privacy en incidenten en diens vervanger, per e-mail en, bij een inbreuk met waarschijnlijk hoog risico, ook telefonisch; buiten Kantoortijden naar het aangewezen noodcontact. Verwerker is voor meldingen bereikbaar via het supportnummer tijdens Kantoortijden en via support@van-oosten.nl en het klantenportaal daarbuiten; in de Hoofdovereenkomst kan een noodlijn buiten Kantoortijden zijn overeengekomen.
- 6.3 De beoordeling of de inbreuk aan de toezichthoudende autoriteit (artikel 33 AVG) en aan betrokkenen (artikel 34 AVG) moet worden gemeld, en het doen van die meldingen, is de verantwoordelijkheid van Verwerkingsverantwoordelijke. Verwerker meldt niet zelfstandig aan de autoriteit of aan betrokkenen, tenzij de wet hem daartoe verplicht of Verwerkingsverantwoordelijke daarom schriftelijk verzoekt. Als Verwerkingsverantwoordelijke een eigen wettelijke meldplicht binnen 24 uur heeft (bijvoorbeeld onder de Cyberbeveiligingswet of de Belgische NIS2-wet), doet Verwerker de eerste melding zo snel mogelijk, ook als de feiten nog onvolledig zijn.
- 6.4 Verwerker documenteert alle inbreuken, met de feiten, gevolgen en genomen maatregelen, bewaart het bewijsmateriaal dat voor onderzoek nodig is en verleent Verwerkingsverantwoordelijke medewerking bij onderzoek, herstel en meldingen.

- 6.5** Verwerker mag bij een acute inbreuk de maatregelen nemen die redelijkerwijs nodig en proportioneel zijn om de gevolgen te beperken, waaronder het blokkeren van accounts en het isoleren van apparaten, en informeert Verwerkingsverantwoordelijke daarover zo snel mogelijk. Voor onomkeerbare maatregelen geldt de regeling in de Hoofdovereenkomst.

Artikel 7. Subverwerkers

- 7.1** Verwerkingsverantwoordelijke geeft Verwerker een algemene schriftelijke toestemming om Subverwerkers in te schakelen. De bij ondertekening ingeschakelde Subverwerkers staan in Bijlage 4.
- 7.2** Verwerker informeert Verwerkingsverantwoordelijke ten minste dertig (30) dagen vóór het inschakelen van een nieuwe Subverwerker of het vervangen van een bestaande Subverwerker, via e-mail aan de contactpersoon en via een actuele lijst in het klantenportaal, met vermelding van de dienst, de verwerkingslocatie en de doorgiftegrond. De nieuwe Subverwerker verwerkt geen persoonsgegevens van Verwerkingsverantwoordelijke vóór het verstrijken van die termijn.
- 7.3** Verwerkingsverantwoordelijke kan binnen de termijn van lid 2 schriftelijk en gemotiveerd bezwaar maken op grond van redelijke, met de bescherming van persoonsgegevens verband houdende redenen. Verwerker reageert binnen tien (10) Werkdagen met een voorstel: aanvullende maatregelen, een alternatieve Subverwerker of het buiten de wijziging houden van de gegevens van Verwerkingsverantwoordelijke. Zolang het bezwaar loopt, verwerkt de nieuwe Subverwerker geen persoonsgegevens van Verwerkingsverantwoordelijke, totdat Partijen een oplossing hebben gevonden of de opzegging van het geraakte deel is ingegaan. Als Partijen binnen dertig (30) dagen na het bezwaar geen oplossing vinden, mag Verwerkingsverantwoordelijke het door de wijziging geraakte deel van de Hoofdovereenkomst opzeggen tegen de datum waarop de Subverwerker wordt ingeschakeld, zonder beëindigingsvergoeding en met terugbetaling van vooruitbetaalde vergoedingen voor dat deel, onverminderd de looptijd van rechtstreeks door Verwerkingsverantwoordelijke afgenomen licenties van derden.
- 7.4** Verwerker legt Subverwerkers dezelfde verplichtingen op als in deze Verwerkersovereenkomst zijn opgenomen, voor zover die relevant zijn voor de door de Subverwerker uitgevoerde verwerking, en blijft jegens Verwerkingsverantwoordelijke verantwoordelijk voor de nakoming door Subverwerkers. Verwerker sluit de vereiste verwerkersovereenkomst met iedere Subverwerker vóórdat die persoonsgegevens van Verwerkingsverantwoordelijke verwerkt en vermeldt de status daarvan in Bijlage 4.
- 7.5** Als Verwerkingsverantwoordelijke rechtstreeks een overeenkomst met een leverancier heeft gesloten (zoals de Microsoft Customer Agreement en het Microsoft DPA), is die leverancier voor de betreffende dienst geen Subverwerker van Verwerker, maar een verwerker van Verwerkingsverantwoordelijke.

Artikel 8. Informatie en audit

- 8.1** Verwerker stelt Verwerkingsverantwoordelijke op verzoek de informatie ter beschikking die nodig is om de nakoming van artikel 28 AVG aan te tonen,

waaronder een beschrijving van de beveiligingsmaatregelen, de subverwerkerslijst met doorgiftegronden en, voor zover beschikbaar, certificeringen en auditrapporten van Subverwerkers.

- 8.2** Verwerkingsverantwoordelijke mag eenmaal per twaalf (12) maanden een audit laten uitvoeren naar de naleving van deze Verwerkersovereenkomst, door zichzelf of door een onafhankelijke, aan geheimhouding gebonden auditor, na een aankondiging van ten minste dertig (30) dagen. Daarnaast mag Verwerkingsverantwoordelijke een audit laten uitvoeren met een verkorte aankondiging van vijf (5) Werkdagen, of bij gerechtvaardigde spoed onmiddellijk, na een inbreuk, op gemotiveerd verzoek van een toezichthoudende autoriteit, of bij een redelijk vermoeden van een wezenlijke tekortkoming. De audit vindt plaats tijdens Kantoortijden, verstoort de bedrijfsvoering van Verwerker zo min mogelijk en strekt zich niet uit tot gegevens van andere klanten van Verwerker.
- 8.3** De kosten van de auditor draagt Verwerkingsverantwoordelijke. De redelijke uren van Verwerker worden tegen het overeengekomen uurtarief in rekening gebracht, met een maximum van acht (8) uur per reguliere audit, tenzij de audit een wezenlijke tekortkoming van Verwerker aantoonst; in dat geval zijn de uren van Verwerker kosteloos. De kostenregeling beperkt het auditrecht niet. Verwerker herstelt geconstateerde tekortkomingen binnen een redelijke, met Verwerkingsverantwoordelijke afgesproken termijn.

Artikel 9. Duur, beëindiging en teruggave

- 9.1** Deze Verwerkersovereenkomst geldt zolang Verwerker persoonsgegevens ten behoeve van Verwerkingsverantwoordelijke verwerkt en eindigt van rechtswege zodra Verwerker alle persoonsgegevens heeft teruggegeven of verwijderd.
- 9.2** Na het einde van de Hoofdovereenkomst geeft Verwerker, naar keuze van Verwerkingsverantwoordelijke, de persoonsgegevens terug in een gangbaar elektronisch formaat en/of verwijdert hij ze, met inachtneming van de exit-regeling in de Hoofdovereenkomst. Na afloop van de daarin overeengekomen exitperiode (of, voor de back-updienst, de ophaalperiode als die later eindigt) verwerkt Verwerker de resterende persoonsgegevens uitsluitend voor veilige verwijdering of voor een concreet toepasselijke wettelijke bewaarplicht. Actieve kopieën worden uiterlijk dertig (30) dagen na het einde van de exitperiode verwijderd; resterende back-upkopieën uiterlijk negentig (90) dagen na het einde van dezelfde exitperiode. Tot verwijdering worden deze kopieën afgeschermd en niet voor andere doeleinden gebruikt. Na een herstel uit back-up worden eerder gegeven wisinstructies opnieuw uitgevoerd. Deze termijnen gelden ook voor Subverwerkers. Op verzoek verstrekt Verwerker een schriftelijke verklaring van verwijdering die de uitvoering bij Subverwerkers omvat.
- 9.3** Gegevens die Verwerker als zelfstandig verwerkingsverantwoordelijke bewaart (Bijlage 1), bewaart Verwerker volgens zijn privacyverklaring en de wettelijke bewaarplichten. Een wettelijke bewaarplicht voor de fiscale administratie rechtvaardigt niet het bewaren van tickets, bijlagen of back-ups van de klantomgeving; die worden volgens lid 2 verwijderd.

Artikel 10. Aansprakelijkheid

- 10.1** Op de aansprakelijkheid van Partijen jegens elkaar uit hoofde van deze Verwerkersovereenkomst is artikel 9 van de Algemene Voorwaarden van Verwerker van toepassing; de daarin opgenomen beperkingen gelden voor de aansprakelijkheid uit de Hoofdovereenkomst en deze Verwerkersovereenkomst gezamenlijk.
- 10.2** Contractuele beperkingen tussen Partijen beperken niet de rechten van betrokkenen en de bevoegdheden van toezichthoudende autoriteiten jegens ieder van Partijen (artikel 82 AVG). Als een Partij de schade van een betrokkene overeenkomstig artikel 82 lid 4 AVG geheel heeft vergoed, kan zij op de andere Partij het deel van de schadevergoeding verhalen dat overeenkomt met het deel van die andere Partij in de aansprakelijkheid voor de schade (artikel 82 lid 5 AVG), binnen de grenzen van artikel 10.1. Voor bestuurlijke boetes geldt verhaal alleen voor zover de wet dat toestaat en de boete het gevolg is van een toerekenbare tekortkoming van de andere Partij. De vrijwaring van artikel 9.8 van de Algemene Voorwaarden is dienovereenkomstig beperkt.

Artikel 11. Overige bepalingen

- 11.1** Wijzigingen van deze Verwerkersovereenkomst zijn alleen geldig als zij schriftelijk zijn overeengekomen. Verwerker mag de Bijlagen aanpassen volgens de artikelen 5.2 en 7.2.
- 11.2** Op deze Verwerkersovereenkomst is Nederlands recht van toepassing. Geschillen worden voorgelegd aan de rechtbank Zeeland-West-Brabant, overeenkomstig de Algemene Voorwaarden. Belgische betrokkenen en Verwerkingsverantwoordelijken behouden hun rechten jegens de Gegevensbeschermingsautoriteit.

Bijlage 1. Rollenmatrix

Verwerking	Gegevens	Rol van Van Oosten Advies	Grondslag en regeling
Contract- en relatiebeheer, facturatie, offertes	Naam, functie, contactgegevens van contactpersonen; bedrijfs- en betaalgegevens	Zelfstandig verwerkingsverantwoordelijke	Uitvoering overeenkomst en wettelijke bewaarplicht; privacyverklaring
Metagegevens van meldingen (tickets): melder, tijdstip, onderwerp, status, bestede tijd	Naam en contactgegevens van de melder, ticketmetagegevens	Zelfstandig verwerkingsverantwoordelijke	Uitvoering overeenkomst en gerechtvaardigd belang (SLA-meting, facturatie); privacyverklaring
Inhoud van meldingen, bijlagen, schermafbeeldingen, logbestanden en andere klantinhoud in tickets	Alle persoonsgegevens die de klant meestuurt, waaronder gegevens van medewerkers en relaties	Verwerker	Deze Verwerkersovereenkomst
Beheer van de Microsoft 365-omgeving en Apparaten namens de klant (accounts, mail, bestanden, beleid, ondersteuning op afstand)	Accountgegevens, inhoud van mail, bestanden, agenda's en chats voor zover toegankelijk	Verwerker	Deze Verwerkersovereenkomst
Monitoring van de klantomgeving en Apparaten (RMM, ITDR, EDR)	Aanmeldlogboeken, apparaatgegevens, beveiligingsgebeurtenissen, IP-adressen	Verwerker	Deze Verwerkersovereenkomst
Back-up en herstel van Microsoft 365 en Entra ID	Volledige inhoud van de beveiligde workloads	Verwerker	Deze Verwerkersovereenkomst; dekking volgens de Hoofdovereenkomst
Documentatie van de klantomgeving (configuratie, inventarisatie, toegangsgegevens)	Namen van gebruikers, apparaatgegevens, toegangsgegevens	Verwerker	Deze Verwerkersovereenkomst
Beveiligingslogboeken van de eigen systemen van Van	Gebruikersnamen en handelingen van medewerkers van	Zelfstandig verwerkingsverantwoordelijke voor de	Gerechtvaardigd belang (beveiliging); privacyverklaring;



Verwerking	Gegevens	Rol van Van Oosten Advies	Grondslag en regeling
Oosten Advies (beheerplatform, documentatieplatform, eigen tenant)	Van Oosten Advies; verwijzingen naar klantobjecten	eigen logboeken; verwerker voor de daarin opgenomen klantgegevens	deze Verwerkersovereenkomst voor klantgegevens
Registratie als Microsoft-partner: klantrelatie, abonnementen, MCA-aanvaarding in Microsoft Partner Center en bij de indirect provider	Bedrijfsgegevens; naam, e-mailadres en telefoonnummer van de persoon die de MCA aanvaardt	Zelfstandig verwerkingsverantwoordelijke (verplicht op grond van de Microsoft-partnervoorwaarden)	Uitvoering overeenkomst en wettelijke/contractuele verplichting; privacyverklaring
Eigen Microsoft 365-omgeving van Van Oosten Advies (mail, agenda, documenten)	Contactgegevens en correspondentie met de klant	Zelfstandig verwerkingsverantwoordelijke; verwerker voor klantinhoud die daarin tijdelijk wordt verwerkt	Privacyverklaring; deze Verwerkersovereenkomst voor klantinhoud

Bijlage 2. Overzicht van verwerkingen

A. Vaste onderdelen

Onderdeel	Beschrijving
Onderwerp van de verwerking	Beheer, ondersteuning en beveiliging van de Microsoft 365-omgeving en werkplekken van Verwerkingsverantwoordelijke volgens het gekozen pakket; back-up en herstel (alleen als het pakket back-up omvat); licentiebeheer; consultancy en maatwerk voor zover daarbij toegang tot persoonsgegevens nodig is
Duur	De looptijd van de Hoofdovereenkomst plus de exitperiode en de verwijdertermijnen van artikel 9
Aard van de verwerking	Toegang, inzage, opslag (back-up, alleen bij het betreffende pakket), herstel, wijziging (accountbeheer), verwijdering, monitoring van beveiligingsgebeurtenissen, ondersteuning op afstand
Doel	Uitvoering van de Hoofdovereenkomst: het werkend, beveiligd en beschikbaar houden van de IT-omgeving
Verwerkingslocatie	EER en landen met adequaatheidsbesluit; uitzonderingen per ontvanger volgens Bijlage 4

B. Klantspecifieke onderdelen (in te vullen in het Opdrachtformulier)

Onderdeel	Standaard	Klantspecifiek
Gekozen pakket en daarmee de verwerkingen (back-up en bewaking alleen bij Compleet en Premium)	Volgens Opdrachtformulier	Volgens Opdrachtformulier
Categorieën betrokkenen	Medewerkers, inhuurkrachten en andere gebruikers van Verwerkingsverantwoordelijke ; contactpersonen van klanten, leveranciers en andere relaties voor zover hun gegevens in de beheerde omgeving voorkomen	Aanvullen: bijvoorbeeld patiënten, cliënten, leerlingen, sollicitanten
Categorieën persoonsgegevens	Identificatie- en contactgegevens, accountgegevens en aanmeldgegevens (gebruikersnaam, aanmeldlogboeken, apparaatgegevens, IP-adres),	Aanvullen: bijvoorbeeld HR-dossiers, financiële gegevens van klanten

Onderdeel	Standaard	Klantspecifiek
	inhoud van e-mail, bestanden, agenda's en chats voor zover aanwezig in de beheerde omgeving en de back-up daarvan, beveiligingsgebeurtenissen	
Bijzondere categorieën, strafrechtelijke gegevens, nationale identificatienummers	Niet beoogd; als zij in mail of documenten voorkomen, gelden de minimale instructies van onderdeel C	Aangeven: niet / incidenteel / structureel, met soort gegevens
Bewaartermijn back-up	Vier (4) jaar voortschrijdend, als in het Opdrachtformulier geen andere termijn is gekozen (gelijk aan Bijlage 1, onderdeel C van de Dienstverleningsovereenkomst)	Iedere termijn van dertig (30) dagen tot dertien (13) jaar of onbeperkt, desgewenst per gegevenssoort (mail, OneDrive, SharePoint)
Bewaartermijn gegevens van vertrokken medewerkers in de omgeving	Verwijdering op instructie van Verwerkingsverantwoordelijke ; mailbox standaard 30 dagen na uitdiensttreding omgezet en daarna volgens instructie	Keuze

C. Minimale instructies voor gevoelige gegevens

Voor bijzondere categorieën van persoonsgegevens, strafrechtelijke gegevens en nationale identificatienummers (zoals BSN of Belgisch rijksregisternummer) geldt, ongeacht of Verwerkingsverantwoordelijke ze heeft gemeld: Verwerker opent de betreffende inhoud alleen als dat voor een concrete opdracht noodzakelijk is; Verwerker kopieert dergelijke gegevens niet naar tickets, chat of documentatie; herstel uit back-up van dergelijke gegevens vindt alleen plaats op instructie van een bevoegde contactpersoon; Verwerker meldt het aan Verwerkingsverantwoordelijke als hij structurele verwerking van dergelijke gegevens constateert die niet is gemeld, zodat aanvullende maatregelen (zoals versleuteling, beperkte toegang of een gegevensbeschermingseffectbeoordeling) kunnen worden afgesproken. Een waarschuwing over bijzondere gegevens vervangt geen passende maatregelen.

Bijlage 3. Beveiligingsmaatregelen

A. Organisatorisch

- › Alle medewerkers en ingeschakelde zelfstandigen van Verwerker zijn contractueel tot geheimhouding verplicht en worden geïnstrueerd over het veilig omgaan met klantgegevens.
- › Toegang tot klantomgevingen en tooling is beperkt tot personen die deze toegang voor hun taak nodig hebben (least privilege) en wordt bij vertrek direct ingetrokken, waarna gedeelde geheimen worden geroteerd.
- › Verwerker houdt een register van verwerkingsactiviteiten en een register van beveiligingsincidenten bij.
- › Verwerker beschikt over een procedure voor het afhandelen en melden van inbreuken (artikel 6) en test die procedure ten minste jaarlijks.
- › Verwerker heeft een beroeps- en bedrijfsaansprakelijkheidsverzekering met dekking voor cyber- en privacyincidenten, met de in het verzekeringscertificaat vermelde limieten.
- › Verwerker werkt uitsluitend met Subverwerkers die beschikken over een geldig ISO 27001-certificaat of een actueel SOC 2-assurancerapport waarvan de reikwijdte de geleverde dienst omvat, of een gelijkwaardig aantoonbaar beveiligingsniveau; Verwerker controleert dit jaarlijks en vermeldt de status in Bijlage 4.

B. Toegang en identiteit

- › Menselijke toegang van Verwerker tot de Microsoft-omgeving van Verwerkingsverantwoordelijke loopt uitsluitend via een tijdgebonden beheerrelatie (GDAP) met de minimaal benodigde rollen; geen permanente Global Administrator-rechten. Machinetoegang loopt via gedocumenteerde app-machtigingen met door Verwerkingsverantwoordelijke gegeven toestemming, volgens de Hoofdovereenkomst.
- › Alle beheerdersaccounts van Verwerker zijn beveiligd met phishingbestendige of app-gebaseerde meervoudige verificatie en voorwaardelijke toegang; beheerdersaccounts zijn gescheiden van de accounts voor dagelijks werk en e-mail.
- › Toegangsgegevens van klanten (waaronder noodtoegangsaccounts) worden uitsluitend opgeslagen in een versleutelde wachtwoordkluis met MFA en toegangslogging; nooit in e-mail, chat of documenten. Verwerkingsverantwoordelijke beschikt daarnaast over eigen, onafhankelijke noodtoegang volgens de Hoofdovereenkomst.
- › Ondersteuning op afstand op apparaten vindt plaats na toestemming van de gebruiker, behalve bij gepland onderhoud buiten werktijd; alle sessies worden gelogd.

C. Techniek

- › Beheer-, monitoring-, documentatie- en back-upplatformen worden geleverd door de in Bijlage 4 genoemde Subverwerkers en zijn beveiligd met MFA, rolgebaseerde toegang en versleuteling in transit (TLS 1.2 of hoger) en in rust (AES-256).

- › Back-ups van Microsoft 365 en Entra ID (alleen bij Compleet en Premium) worden opgeslagen in de Europese Unie, gescheiden van de productieomgeving, met de door de leverancier contractueel bevestigde bescherming tegen wijziging of verwijdering, en worden ieder kwartaal getest door een proefherstel.
- › De werkplekken van Verwerker zijn versleuteld, worden centraal beheerd, zijn voorzien van endpointbeveiliging en worden automatisch bijgewerkt.
- › Beheerhandelingen in klantomgevingen worden gelogd in het beheerplatform van Verwerker en, waar de licentie dat toelaat, in de auditlogboeken van Microsoft 365 van Verwerkingsverantwoordelijke.
- › In de omgeving van Verwerkingsverantwoordelijke past Verwerker de beveiligingsbaseline toe die in de Hoofdovereenkomst voor het gekozen pakket is overeengekomen.

D. Continuïteit

- › Documentatie van klantomgevingen wordt versleuteld opgeslagen in het documentatieplatform van Verwerker met een dagelijkse back-up.
- › Bij uitval van Verwerker behoudt Verwerkingsverantwoordelijke via zijn eigen noodtoegangssaccounts toegang tot zijn omgeving; de exit-regeling van de Hoofdovereenkomst voorziet in overdracht.



Bijlage 4. Subverwerkers en doorgiften

Stand per 1 oktober 2026. De actuele lijst, met de datum van de laatste controle van certificeringen, verwerkersovereenkomsten en DPF-status, staat in het klantenportaal van Verwerker en wordt op verzoek verstrekt. Wijzigingen worden aangekondigd volgens artikel 7.2. Een Subverwerker verwerkt geen gegevens van Verwerkingsverantwoordelijke voordat de verwerkersovereenkomst met die Subverwerker is gesloten en de verwerkingslocatie en doorgiftegrond zijn vastgesteld.

A. Subverwerkers in de klantketen

Subverwerker (rechtspersoon)	Dienst en rol	Verwerkte gegevens
NinjaOne, LLC (Tampa, Florida, VS; Europese affiliate NinjaOne GmbH, Berlijn)	Beheer en monitoring van apparaten (RMM), ondersteuning op afstand, ticketsysteem, documentatie, back-up van Microsoft 365 en Entra ID (alleen bij Compleet en Premium)	Gebruikers- en apparaatgegevens, ticketinhoud, documentatie van de omgeving, back-upgegevens (inhoud van mail, bestanden, chats)
Huntress Labs Incorporated (Columbia, Maryland, VS)	24/7 geautomatiseerde bewaking van Microsoft 365-accounts (ITDR) en van apparaten (EDR, alleen Premium), security awareness-training (alleen Premium)	Aanmeldlogboeken, accountgegevens, beveiligingsgebeurtenissen van apparaten, trainingsresultaten van gebruikers
CyberDrain B.V. (KvK 86594893, Hoogvliet Rotterdam; gehoste CIPP)	Beheerplatform voor Microsoft 365-omgevingen: uitrol en bewaking van beveiligingsinstellingen, gebruikersbeheer, rapportages	Gebruikersnamen, licentie- en configuratiegegevens, beveiligingsstatus
Proton AG	Wachtwoordkluis voor toegangsgegevens van klantomgevingen	Toegangsgegevens (end-to-end versleuteld; Proton heeft geen toegang tot de inhoud)

Subverwerker	Verwerkingslocatie en supporttoegang	Doorgiftegrond	DPA-status en certificering
NinjaOne	Beheerplatform: EU-instantie bij Amazon Web Services in Duitsland; back-upgegevens: AWS-datacenter Frankfurt of Dublin, afhankelijk van de regio van het partneraccount	Verwerking in de EU; voor supporttoegang: EU-VS Data Privacy Framework (certificering NinjaOne, LLC; status wordt vóór de eerste verwerking en daarna jaarlijks gecontroleerd),	NinjaOne Data Processing Addendum versie 8 juni 2026; ISO 27001:2022 en SOC 2 Type II (rapport onder NDA via het NinjaOne Trust Center)



Subverwerker	Verwerkingslocatie en supporttoegang	Doorgiftegrond	DPA-status en certificering
	(bevestigd in het activeringsverslag); supporttoegang mogelijk vanuit de VS en, via de subverwerker Exypnox, de Filipijnen	subsidiar SCC module 3 uit de NinjaOne-DPA	
Huntress	Verenigde Staten (Amazon Web Services en Microsoft Azure); SOC-analisten in de VS; de leverancier biedt geen EU-verwerkingslocatie	EU-VS Data Privacy Framework (certificering Huntress Labs Incorporated; status wordt vóór de eerste verwerking en daarna jaarlijks gecontroleerd) en SCC uit de Huntress-DPA, met aanvullende maatregelen (versleuteling in transit en in rust)	Huntress Data Processing Addendum via het Huntress Trust Center; SOC 2 Type II (rapport via het Trust Center)
CyberDrain B.V.	Nederland; hosting in Microsoft Azure in de tenant van CyberDrain B.V.; de Azure-regio wordt door CyberDrain schriftelijk bevestigd en aan Verwerkingsverantwoordelijke gemeld vóór de eerste verwerking	Verwerking in de EU	Verwerkersovereenkomst met CyberDrain B.V., gesloten vóór de eerste verwerking; certificering: geen (ISO 27001 in voorbereiding volgens CyberDrain); het gelijkwaardige beveiligingsniveau is vastgelegd in de beveiligingsdocumentatie van CyberDrain (docs.cipp.app, security and compliance) en wordt jaarlijks door Verwerker beoordeeld
Proton AG	Zwitserland; opslag in Zwitserland, Duitsland en Noorwegen (EER)	Adequaatheidsbesluit Zwitserland (Beschikking 2000/518/EG, bevestigd in de evaluatie van 15 januari 2024)	Proton DPA versie 10 februari 2026, onderdeel van de zakelijke voorwaarden; ISO 27001 (sinds 2 mei 2024) en SOC 2 Type II (juli 2025)

**B. Ontvangers buiten de klantketen (eigen verwerkingen van Verwerker; ter informatie)**

Ontvanger	Dienst	Gegevens	Toelichting
Microsoft Ireland Operations Ltd.	Microsoft Partner Center (registratie van de klantrelatie, abonnementen en MCA-aanvaarding)	Bedrijfs- en contactgegevens, abonnementsgegevens	Eigen verwerking van Verwerker als Microsoft-partner; Microsoft is daarvoor verwerker van Verwerker onder het Microsoft DPA; EU Data Boundary volgens de Microsoft-documentatie met de daarin beschreven uitzonderingen
Crayon B.V., Amsterdam (indirect provider Microsoft CSP)	Licentieadministratie en facturatie van Microsoft-abonnementen	Bedrijfsgegevens, gegevens van de persoon die de MCA aanvaardt, abonnementsgegevens	Eigen verwerking; verwerking in de EU
Microsoft Ireland Operations Ltd.	Microsoft Dynamics 365 Business Central en Microsoft 365 (eigen administratie en communicatie van Verwerker)	Contact- en factuurgegevens, correspondentie	Eigen verwerking; privacyverklaring
WhatsApp Ireland Limited (Meta), Dublin	WhatsApp Business-app (supportkanaal)	Telefoonnummer, naam en berichtinhoud van de melder (berichten zijn end-to-end versleuteld; metagegevens worden door WhatsApp verwerkt)	Eigen verwerking; doorgifte naar WhatsApp LLC en Meta Platforms, Inc. (VS) op basis van het EU-VS Data Privacy Framework en SCC's volgens het WhatsApp Business Data Transfer Addendum; Verwerkingsverantwoordelijke en zijn gebruikers delen via dit kanaal geen wachtwoorden of gevoelige gegevens; berichten worden na afhandeling in het ticketsysteem vastgelegd en uit WhatsApp verwijderd volgens de privacyverklaring

C. Microsoft-clouddiensten van Verwerkingsverantwoordelijke

Voor Microsoft 365, Entra ID, Intune en Defender is Microsoft de verwerker van Verwerkingsverantwoordelijke op grond van de Microsoft Customer Agreement en het Microsoft Products and Services Data Protection Addendum (www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA). Microsoft verwerkt en bewaart klantgegevens binnen de EU Data Boundary volgens de reikwijdte en de gedocumenteerde uitzonderingen die Microsoft publiceert (learn.microsoft.com/privacy/eudb). De subverwerkers van Microsoft staan op de lijst die Microsoft publiceert via het Microsoft Trust Center.

D. Vervalprocedure

Als voor een ontvanger een doorgiftegrond vervalt (bijvoorbeeld doordat de DPF-inschrijving eindigt of het adequaatheidsbesluit ongeldig wordt verklaard), past Verwerker artikel 3.3 toe: binnen dertig (30) dagen een andere geldige waarborg (SCC met aanvullende maatregelen) of opschorting van de doorgifte, met kennisgeving aan Verwerkingsverantwoordelijke. De procedure tegen het EU-VS Data Privacy Framework (Gerecht EU, T-553/23, Latombe, hoger beroep C-703/25 P) wordt door Verwerker gevolgd; het adequaatheidsbesluit blijft geldig totdat het Hof anders beslist.