

Verwerkersovereenkomst

Norwin AI Platform

Versie 1.7 · Definitief · 12 oktober 2026

Bijlage 4 (Module AI-verwerking, versie 1.4) is een apart geaccepteerde module. Wijzigingen in versie 1.7: Bijlage 4, artikel 4.4 (het AI-model: een model van Anthropic via AWS Bedrock in de EER, de actuele modelnaam op de pagina Datalocatie, een wijziging van het model 30 dagen vooraf aangekondigd, met verwijzing naar artikel 4.5, 4.8, 4.11, 4.12 en 5.2) en artikel 4.12(e) (elke wijziging van het model is wezenlijk), de verwijzing in Bijlage 3 (geen vaste modelnaam meer) en artikel 3.5 (verlenging van de toegang in plaats van een nieuwe Keuze). Chat met AI blijft uit tot een Admin Bijlage 4 versie 1.4 accepteert. Versie 1.6 blijft de vorige versie.

Inhoud

	Partijen	2
Artikel 1	Definities	2
Artikel 2	Onderwerp en instructies	2
Artikel 3	Geheimhouding en toegang van Staff	3
Artikel 4	Beveiliging	4
Artikel 5	Subverwerkers	4
Artikel 6	Doorgifte	5
Artikel 7	Rechten van betrokkenen	6
Artikel 8	Datalekken	6
Artikel 9	Bijstand en informatie	6
Artikel 10	Duur, einde, teruggave en verwijdering	7
Artikel 11	Aansprakelijkheid	7
Artikel 12	Rangorde en recht	8
Bijlage 1	Beschrijving van de verwerking	9
Bijlage 2	Technische en organisatorische maatregelen	11
Bijlage 3	Subverwerkers	14
Bijlage 4	Module AI-verwerking	20
Deel A	AI van Verwerker	20
Deel B	eigen AI-koppeling van de Klant	25
	Wijzigingshistorie	26

Partijen

1. De klant, zoals geregistreerd bij de aanmelding (naam, KvK-nummer, adres):
"Verwerkingsverantwoordelijke".
2. Norwin AI B.V., Rivium Eerste Straat 147J, 2909 LE Capelle aan den IJssel, KvK 42113670, btw NL869791795B01: "Verwerker".

Deze verwerkersovereenkomst ("VWO") is deel van de overeenkomst voor het gebruik van het Norwin AI Platform ("Hoofdovereenkomst"). Ze komt tot stand bij elektronische acceptatie.

Artikel 1

Definities

Begrippen hebben de betekenis uit de Verordening (EU) 2016/679 ("AVG"). "Klantgegevens" zijn alle persoonsgegevens die Verwerker verwerkt als onderdeel van de dienstverlening binnen de workspace van Verwerkingsverantwoordelijke. "Subverwerker" is een derde die Verwerker inschakelt om Klantgegevens te verwerken. "Staff" zijn medewerkers van Verwerker. "Admin" is een gebruiker met de rol workspace-admin.

Artikel 2

Onderwerp en instructies

- 2.1 Verwerker verwerkt Klantgegevens alleen in opdracht en volgens de gedocumenteerde instructies van Verwerkingsverantwoordelijke, ook bij doorgifte naar een derde land. Dat geldt niet als het Unierecht of het recht van een lidstaat hem tot verwerking verplicht. Dan informeert Verwerker Verwerkingsverantwoordelijke vooraf, tenzij dat recht die kennisgeving verbiedt (art. 28 lid 3 onder a AVG).
- 2.2 De Hoofdovereenkomst, deze VWO en de instellingen die Verwerkingsverantwoordelijke in het Platform kiest, vormen samen de instructies. Bijlage 1 beschrijft de verwerking.
- 2.3 Verwerker meldt het direct als een instructie naar zijn oordeel in strijd is met de AVG of andere wetgeving (art. 28 lid 3, slot, AVG).
- 2.4 Verwerker gebruikt Klantgegevens niet voor eigen doeleinden, behalve wat Bijlage 1 onder "Eigen doeleinden van Verwerker" uitdrukkelijk noemt: (a) de eigen klantrelatie en facturatie; (b) de beperkte bewaring van gepseudonimiseerde audit-gebeurtenismetadata na het einde van de Hoofdovereenkomst, voor rechtsvorderingen (artikel 10.3); (c) het bewijs van acceptatie van deze VWO en de Hoofdovereenkomst. Voor die verwerkingen is Verwerker zelf verwerkingsverantwoordelijke, en daarvoor geldt de Privacyverklaring. Verwerker anonimiseert en aggregeert Klantgegevens op instructie van Verwerkingsverantwoordelijke, als verwerker, om gebruiksstatistieken te maken (Hoofdovereenkomst art. 9.2). Wat daaruit ontstaat, is niet tot Verwerkingsverantwoordelijke of een persoon te herleiden. Verwerker publiceert die statistieken of gebruikt ze buiten Verwerker alleen als ze op ten minste 5 workspaces berusten. Accountbeveiliging, login en misbruikdetectie horen bij de dienstverlening van het Platform zelf. Ze zijn geen eigen doel van Verwerker.
- 2.5 Verwerker gebruikt Klantgegevens **niet om generatieve AI-modellen te trainen**. Hij staat dat ook zijn Subverwerkers niet toe. Voor de beveiligings- en spamfilters van de e-maildienst geldt de nuance uit Bijlage 3.

Artikel 3

Geheimhouding en toegang van Staff

- 3.1 Verwerker zorgt dat personen die Klantgegevens mogen verwerken, zich tot geheimhouding hebben verbonden of onder een wettelijke geheimhoudingsplicht vallen (art. 28 lid 3 onder b AVG).
- 3.2 **Proactieve begeleiding.** Proactieve begeleiding staat standaard aan. Een Admin kan deze uitzetten onder Instellingen. Staff kijkt dan alleen mee op verzoek van de Klant, bij support of bij een beveiligingsincident. Staff gebruikt wat hij ziet uitsluitend om de Klant te helpen bij het gebruik van het Platform en bij zijn AI-transformatie. Staff kopieert geen inhoud buiten het Platform, legt geen Workspace-inhoud vast in eigen CRM of andere systemen, beoordeelt geen individuele Gebruikers en doet geen aanbod voor betaalde diensten op grond van wat hij zag, tenzij de Klant daarom vraagt.
- De instelling van de Admin is de instructie van Verwerkingsverantwoordelijke (art. 28 lid 3 onder a AVG). Verandert de Admin niets, dan geldt de standaardinstelling.
 - De opt-out is een organisatorische maatregel, geen technische blokkade. Staff kan technisch alle Workspace-inhoud lezen, behalve chatinhoud (artikel 3.3), persoonlijke instructies voor de AI (Bijlage 4, artikel 4.16) en geletterdheidsgegevens per persoon (hieronder). Bij elke toegang kiest staff een reden. Het Platform legt die keuze vast. Verwerker controleert de gekozen redenen wanneer er een vermoeden of aanleiding voor is.
 - Via het Platform legt Verwerker per staff-lid per workspace één gebeurtenis per 30 minuten vast, met de reden. Dat geldt voor workspaces waarvan de medewerker geen lid is. De Admin ziet dit in de audit-trail. Toegang buiten het Platform valt onder artikel 3.4.
 - Support en beveiligingsincidenten blijven altijd mogelijk, ook als de Admin proactieve begeleiding uitzet.
 - Een lopende offerte of adviesopdracht van Verwerkingsverantwoordelijke aan Verwerker (Hoofdovereenkomst art. 6.5) geldt als verzoek van Verwerkingsverantwoordelijke. Zonder lopende offerte of opdracht gebruikt Staff die reden niet.
 - Doet een staffmedewerker toch een aanbod voor betaalde diensten op grond van wat hij zag, zonder dat Verwerkingsverantwoordelijke daarom vroeg, dan volgt een interne disciplinaire maatregel. Deze regel is organisatorisch; het Platform kan hem niet technisch afdwingen.
 - Voor chat tussen collega's geldt in plaats hiervan artikel 3.3.
 - Staff heeft geen leesrechten op geletterdheidsgegevens zonder zichzelf eerst toe te voegen als lid van de workspace; dat toevoegen zelf wordt vastgelegd en gemeld aan de Admin. Geletterdheidsgegevens zijn hier de gegevens per persoon: toegewezen e-learnings, "afgerond" met datum en het niveau van een medewerker. Dat geldt ook als staff zich met de rol Admin toevoegt. De Admin ziet het toevoegen in de audit-trail onder Instellingen > Toegang en als melding in het Platform. De opzet van programma's (naam, link, niveaus en categorieën) kan staff wel lezen. Toegang buiten het Platform valt onder artikel 3.4.
- 3.3 **Chat tussen collega's.** Staff heeft geen toegang tot de inhoud van chatberichten tussen gebruikers via het Platform, tenzij de staff-medewerker zelf deelnemer is aan die chat. Hetzelfde geldt voor gesprekken met de AI-assistent (Bijlage 4, artikel 4.9) en voor persoonlijke instructies (Bijlage 4, artikel 4.16). Dit is technisch afgedwongen met Row Level Security (artikel 4, Bijlage 2). Voor chatthreads legt het Platform alleen vast: workspace, aanmaker, tijdstip en aantal deelnemers, nooit titel, inhoud of overige deelnemers (thread_created). Staff heeft geen toegang tot chatinhoud, maar kan dit beperkte auditgegeven zien als onderdeel van het generieke beveiligingslog. Chat en de bijbehorende

audit-trail kunnen binnen de organisatie van Verwerkingsverantwoordelijke onder het instemmingsrecht van de ondernemingsraad vallen (art. 27 WOR). Verwerkingsverantwoordelijke beoordeelt dat zelf.

3.4 Toegang tot databases.

- Verwerker gebruikt handmatige toegang tot Klantgegevens buiten het Platform, rechtstreeks op databaseniveau, alleen bij een beveiligingsincident of op schriftelijk verzoek van Verwerkingsverantwoordelijke. Verwerker legt elke handmatige toegang vast in een logboek: wie, wanneer, welke workspace en waarom.
- Voor chatinhoud en voor persoonlijke instructies loopt die toegang via de gelogde procedure van artikel 7, die draait bij GitHub (Bijlage 3).
- Buiten dit artikel valt het routinematig toepassen van databasemigraties en het uitrollen van de applicatie en haar functies via CI/CD, zoals Bijlage 3 beschrijft (de Supabase-GitHub-koppeling voor databasemigraties; de uitrol van Edge Functions en het beheer van de Vercel-configuratie, lokaal door Verwerker). Dat is een vooraf geïnstrueerde categorie, onderdeel van de dienstverlening (Bijlage 1). Zo'n migratie of uitrol wijzigt de structuur of de programmatuur van het Platform en is niet bedoeld om Klantgegevens in te zien.

3.5 **Partnertoegang tot een project.** Geeft de Verwerkingsverantwoordelijke via een Keuze een Partner toegang tot een project, dan is dat een instructie (artikel 2.2). Verwerker verzorgt alleen de technische toegang, beperkt tot dat project, en legt de Keuze, de intrekking en de acceptatie van het model door beide partijen vast. De toegang vervalt automatisch 6 maanden na de Keuze, tenzij de Verwerkingsverantwoordelijke de toegang vóór het verval verlengt (Algemene Voorwaarden artikel 6.13.5(b)). De Partner is geen Subverwerker van Verwerker. De Verwerkingsverantwoordelijke sluit met de Partner een verwerkersovereenkomst, standaard het Model-VWO van het Platform. Beide accepteren dat in het Platform, uitdrukkelijk: de Verwerkingsverantwoordelijke met een aparte bevestiging bij de Keuze, de Partner bij zijn aanmelding en bij elke nieuwe versie. Verwerker is daarbij geen partij. Is Norwin AI B.V. zelf de Partner, dan is zij partij bij het model, als verwerker van de Verwerkingsverantwoordelijke in haar hoedanigheid van Partner; voor de verwerking binnen de Opdracht gaat dan het model voor deze VWO. De Partner verwerkt en heeft toegang alleen binnen de EER. Verwerker beoordeelt de Partner niet en is niet aansprakelijk voor de verwerking door de Partner. Verwerker blijft verantwoordelijk voor de technische afscherming van alle andere gegevens.

Artikel 4

Beveiliging

- 4.1 Verwerker neemt de technische en organisatorische maatregelen uit Bijlage 2 (art. 32 AVG).
- 4.2 Verwerker mag de maatregelen aanpassen, mits het beschermingsniveau niet daalt.

Artikel 5

Subverwerkers

- 5.1 Verwerkingsverantwoordelijke geeft algemene schriftelijke toestemming voor de Subverwerkers uit Bijlage 3 (art. 28 lid 2 AVG).
- 5.2 Een voorgenomen toevoeging of vervanging meldt Verwerker minstens 30 dagen vooraf, per e-mail aan de workspace-admin(s) en op de pagina "Datalocatie en toegang door overheden" (/datalocatie in het Platform). Verwerkingsverantwoordelijke kan binnen die termijn gemotiveerd bezwaar maken. Lossen

partijen het bezwaar niet op, dan kan Verwerkingsverantwoordelijke de Hoofdovereenkomst kosteloos opzeggen per de ingangsdatum van de wijziging. Meldt een Subverwerker zelf korter dan 30 dagen vooraf, dan geeft Verwerker de melding door binnen 5 werkdagen na ontvangst. Verwerkingsverantwoordelijke kan dan de Hoofdovereenkomst kosteloos per direct opzeggen.

- 5.3 Verwerker legt elke Subverwerker schriftelijk ten minste de kernverplichtingen van deze VWO op, met de afwijkingen die Bijlage 3 per Subverwerker benoemt. Hij blijft volledig aansprakelijk voor de nakoming door de Subverwerker (art. 28 lid 4 AVG).
- 5.4 Klantgegevens worden opgeslagen in de EU. Verwerking en toegang van buiten de EER vinden plaats voor ondersteunende functies, onder de waarborgen in Bijlage 3. Voorbeelden zijn een wereldwijd netwerk, support en onderhoud, en beheerworkflows. Heeft een Subverwerker (of zijn moedermaatschappij, of een van zijn eigen subverwerkers) een vestiging buiten de EER, zodat buitenlandse autoriteiten toegang kunnen vorderen of toegang van buiten de EER plaatsvindt, dan vermeldt Verwerker dat in Bijlage 3, samen met het doorgiftemechanisme en de aanvullende maatregelen (hoofdstuk V AVG).
- 5.5 **AI-module.** Amazon Web Services EMEA SARL (Bijlage 3) verwerkt alleen Klantgegevens van een workspace waarvan de Admin de Module AI-verwerking (versie 1.2 of hoger, Bijlage 4) heeft geaccepteerd en chat met AI heeft ingeschakeld, en alleen voor gesprekken met de AI van Verwerker (Deel A). Met die acceptatie geeft Verwerkingsverantwoordelijke specifieke schriftelijke toestemming voor die Subverwerker (toestemming als bedoeld in artikel 28 lid 2 AVG; geen toestemming als grondslag in de zin van artikel 6 of 7 AVG) voor de doeleinden van Bijlage 4. Voor deze Subverwerker en deze workspace geldt daarom de aankondigingstermijn van artikel 5.2 niet. Voor een latere toevoeging of vervanging van een Subverwerker voor deze module geldt artikel 5.2 wel.
- 5.6 **Eigen AI-koppeling.** Een AI-aanbieder die de Verwerkingsverantwoordelijke zelf koos (Bijlage 4, Deel B) is geen Subverwerker. De artikelen 5.2 en 5.3 gelden niet voor hem. Verwerker stuurt gegevens alleen naar een Europees eindpunt van die aanbieder (Bijlage 4, artikel 4.23).

Artikel 6

Doorgifte

- 6.1 Verwerker geeft Klantgegevens niet door naar een land buiten de EER zonder passende waarborgen in de zin van hoofdstuk V AVG en zonder voorafgaande vermelding in Bijlage 3.
- 6.2 Verzoekt een overheidsinstantie buiten de EER om Klantgegevens, dan:
- informeert Verwerker Verwerkingsverantwoordelijke, voor zover dat wettelijk mag;
 - betwist Verwerker het verzoek als daar redelijke gronden voor zijn;
 - verstrekt Verwerker niet meer dan strikt noodzakelijk (vgl. art. 48 AVG).
- 6.3 **Terugval.** Steunt een doorgifte op het EU-VS Data Privacy Framework (DPF), en wordt het DPF geschorst of vernietigd, of vervalst de certificering van de Subverwerker, dan gelden voor die doorgifte vanaf dat moment de standaardcontractbepalingen (SCC's) die Bijlage 3 voor die Subverwerker noemt. Verwerker stelt dan voor die doorgifte een doorgiftetoets (TIA) op.

Artikel 7

Rechten van betrokkenen

Verwerker helpt Verwerkingsverantwoordelijke met passende maatregelen om verzoeken van betrokkenen te beantwoorden (art. 28 lid 3 onder e AVG). Dit geldt ook voor verwijderingsverzoeken die de audit-trail raken; zie artikel 10.3. Voor chatinhoud, ook die van gesprekken met de AI-assistent, en voor persoonlijke instructies voert Verwerker, omdat hij die inhoud niet uit zichzelf inziet (artikel 3.3), op schriftelijke instructie van Verwerkingsverantwoordelijke een gelogde databasequery uit om een verzoek van een betrokkene te beantwoorden. Verwerker voert die query uit via een geautomatiseerde procedure bij GitHub (Bijlage 3). De uitvoer is versleuteld en staat maximaal één dag bij GitHub. In de metadata van de uitvoering staan het workspace-ID, het ID van de betrokkene, het dossiernummer en de reden, geen chatinhoud. Verwerker beschrijft de procedure schriftelijk en logt elke uitvoering. Verwerker richt de procedure in (omgevingen, databaserol en sleutel) voordat hij een eerste verzoek over chatinhoud of persoonlijke instructies uitvoert. Verzoeken die Verwerker rechtstreeks ontvangt, stuurt hij zonder onnodige vertraging door. Een redactie in een gesprek met de AI-assistent vervangt ook de titel van dat gesprek.

Artikel 8

Datalekken

- 8.1 Verwerker meldt een inbreuk in verband met persoonsgegevens zonder onredelijke vertraging nadat hij ervan kennis heeft genomen, aan de Admin(s), per e-mail (Hoofdovereenkomst art. 19.2; art. 33 lid 2 AVG). Dat geldt vanaf het moment dat Verwerker kennis heeft, ook als een Subverwerker later meldt. Verwerker streeft ernaar binnen 48 uur te melden. Bijlage 2, punt 12, noemt het contactpunt.
- 8.2 De melding bevat de informatie uit art. 33 lid 3 AVG, voor zover die beschikbaar is. Wat nog ontbreekt, volgt in fasen.
- 8.3 Het besluit om te melden aan de Autoriteit Persoonsgegevens of aan betrokkenen ligt bij Verwerkingsverantwoordelijke.

Artikel 9

Bijstand en informatie

- 9.1 Verwerker helpt Verwerkingsverantwoordelijke bij het nakomen van de verplichtingen uit art. 32 tot en met 36 AVG (beveiliging, datalekken, DPIA's en voorafgaande raadpleging), rekening houdend met de informatie waarover hij beschikt (art. 28 lid 3 onder f AVG). Voor de Module AI-verwerking levert Verwerker op verzoek de beschrijving van de verwerking die Verwerkingsverantwoordelijke nodig heeft voor een DPIA.
- 9.2 Verwerker stelt alle informatie beschikbaar die nodig is om de naleving aan te tonen, en werkt mee aan audits (art. 28 lid 3 onder h AVG):
 - eerst via documentatie en de rapporten van de interne security-test (die heet uitdrukkelijk geen onafhankelijke test);
 - daarna via een audit door een onafhankelijke deskundige, maximaal 1× per jaar, met 30 dagen aankondiging, op kosten van Verwerkingsverantwoordelijke tenzij er een wezenlijke tekortkoming blijkt;
 - Verwerkingsverantwoordelijke kiest de auditor;

- een extra audit binnen hetzelfde jaar is toegestaan na een datalek dat Verwerkingsverantwoordelijke raakt, of op verzoek van een toezichthoudende autoriteit. Bij spoed geldt de aankondigingstermijn van 30 dagen dan niet.

Artikel 10

Duur, einde, teruggave en verwijdering

10.1 Deze VWO loopt zo lang Verwerker Klantgegevens verwerkt.

10.2 Na het einde van de Hoofdovereenkomst:

- kan Verwerkingsverantwoordelijke gedurende 30 dagen zijn Klantgegevens exporteren in een gestructureerd, gangbaar en machineleesbaar formaat;
- verwijdt Verwerker daarna de Klantgegevens binnen 30 dagen, inclusief kopieën, tenzij het Unierecht of het lidstatelijk recht opslag verplicht (art. 28 lid 3 onder g AVG);
- gesprekken met de AI-assistent horen bij de Klantgegevens en worden op dezelfde termijn verwijderd;
- het organisatieprofiel verwijdt Verwerker op dezelfde termijn; persoonlijke instructies verdwijnen zodra het lidmaatschap van de Gebruiker eindigt (Bijlage 4, artikel 4.16);
- verwijdt Verwerker de inlogaccounts binnen dezelfde termijn;
- verdwijnt data uit back-ups uiterlijk na afloop van de back-upcyclus van 7 dagen.

10.3 **Audit-trail na het einde.** Na het einde bewaart Verwerker van de audit-trail alleen gebeurtenismetadata: type gebeurtenis, tijdstip, workspace-ID en een vervangend gebruikers-ID. Verwerker vervangt het gebruikers-ID door een willekeurig ID per workspace. Er is geen koppeling met het inlogaccount. Dit is pseudonimisering, geen anonimisering. Verwerker bewaart geen koppeltabel tussen het oude en het vervangende ID. Veldinhoud, dat zijn de oude en nieuwe waarden van gewijzigde gegevens, leegt Verwerker uiterlijk 30 dagen na het einde van de Hoofdovereenkomst. Die kunnen klanthinoud bevatten, zoals namen, prijzen en bedrijfsgeheimen. De metadata blijft maximaal 5 jaar na het einde van de Hoofdovereenkomst bewaard, voor het vastleggen, uitoefenen of verdedigen van rechtsvorderingen (verjaring, art. 3:307/3:310 BW), met uitzondering van gebeurtenissen over Bedrijfsgegevens (Algemene Voorwaarden artikel 2.7), die Verwerker uiterlijk 30 dagen na het einde verwijdt. Verwerkingsverantwoordelijke geeft hiervoor in deze VWO uitdrukkelijk instructie (art. 28 lid 3 onder a AVG). Voor deze beperkte bewaring is Verwerker zelf verwerkingsverantwoordelijke (art. 17 lid 3 onder e AVG), zoals Bijlage 1 vermeldt.

Artikel 11

Aansprakelijkheid

De aansprakelijkheid van partijen onder deze VWO volgt de Hoofdovereenkomst, met dezelfde limiet, ook voor schade uit datalekken. Dit laat de rechten van betrokkenen onder art. 82 AVG onverlet.

Artikel 12

Rangorde en recht

Bij strijd gaat deze VWO vóór de Hoofdovereenkomst. Nederlands recht is van toepassing. De rechter uit de Hoofdovereenkomst is bevoegd.

Bijlage 1

Beschrijving van de verwerking

Onderdeel	Inhoud
Aard en doel	Het leveren van het Norwin AI Platform: kansenkaart, kansen en projecten beheren, samenwerken in een workspace, gebruikers en rollen beheren, uitnodigen, wijzigingen vastleggen (audit-trail), chat tussen collega's binnen de workspace (geen AI-functie; voor chatthreads legt het platform alleen vast: workspace, aanmaker, tijdstip en aantal deelnemers, nooit titel, inhoud of overige deelnemers; Norwin AI-staff heeft geen toegang tot chatinhoud, maar kan dit beperkte auditgegevens zien als onderdeel van het generieke beveiligingslog), optionele chat met AI (Module AI-verwerking, Bijlage 4), met een organisatieprofiel, persoonlijke instructies, kansen en projecten als context en voorstellen voor kansen en taken, via de AI van Verwerker (Deel A) of een eigen AI-koppeling van de Klant (Deel B); geen gespreksinhoud, profieltekst of instructietekst in de audit-trail, en proactieve begeleiding van de workspace door Staff (standaard aan, uit te zetten door de Admin; artikel 3.2). AI-geletterdheid: e-learnings toewijzen en vastleggen dat ze zijn afgerond, met datum; niveaus; en het registreren van een extern programma (naam, aanbieder, link); de geletterdheidsfuncties van de Algemene Voorwaarden artikel 4.8: een eigen programma met categorieën en niveaus, een verklaring van de Admin, een extern programma en een niveau per team. Registreren en opslaan van een AI-beleid en een toolregister (de aanvrager van een tool is een persoon; de status is het oordeel van de Klant). Het starten van een Sjabloon uit de bibliotheek (de kopie is Klantgegevens). Technische toegang van een Partner tot één project na een Keuze (artikel 3.5). Het routinematig toepassen van databasemigraties en het uitrollen van de applicatie via CI/CD (artikel 3.4, Bijlage 3). Verder: anonimiseren en aggregeren van Klantgegevens tot gebruiksstatistieken, op instructie, extern alleen gebruikt vanaf 5 workspaces (artikel 2.4)
Categorieën betrokkenen	Gebruikers van de klant (admins, members), ook wanneer zij met de AI-assistent chatten; medewerkers van de klant die worden uitgenodigd of genoemd; contactpersonen van de klant; personen die in vrije tekst worden genoemd (bijv. in projectomschrijvingen)
Categorieën persoonsgegevens	Naam, zakelijk e-mailadres, rol en lidmaatschap, gebruikers-ID; bij inloggen met een identiteitsprovider ook de naam van de provider, de vaste account-ID van de Gebruiker bij de provider en, bij Microsoft, de tenant-ID; andere gegevens die de provider meestuurt bewaart Verwerker niet (geen profielfoto, geen token van de provider); activiteit en wijzigingshistorie (wie, wanneer, welk veld, oude en nieuwe waarde); inhoud die de klant zelf invoert; profielfoto's van gebruikers en bedrijfslogo's (privé opslag); chatberichten tussen gebruikers (inhoud, deelnemers, tijdstip; Verwerker leest deze niet, behalve volgens artikel 3.3 en 3.4); inhoud van gesprekken met de AI-assistent (invoer en antwoorden; per aanroep gaan maximaal 40 eerdere berichten mee, Bijlage 4, artikel 4.3; Verwerker leest deze niet, behalve volgens artikel 3.3, 3.4 en 7); het organisatieprofiel (vrije tekst van de Admin, maximaal 2.000 tekens; alle Gebruikers van de workspace en Staff kunnen het lezen; Bijlage 4, artikel 4.15); persoonlijke instructies (vrije tekst van de Gebruiker, maximaal 1.000 tekens, privé; Verwerker leest ze niet, behalve volgens artikel 3.3, 3.4 en 7; Bijlage 4, artikel 4.16); per kans of project die een Gebruiker als context meestuurt: titel, fase, of het een lighthouse is, plaats op de kansenkaart, aantal taken per status, verwachte uitwerking en beschrijving (vrije tekst, kan persoonsgegevens bevatten; geen namen of ID's van aanmakers, beheerders of toegewezen personen; Bijlage 4, artikel 4.17); voorstellen van de AI in een gesprek; wat een Partner na de Keuze ziet (projectnaam en -omschrijving, fase, taken, bedrijfsnaam, één contactpersoon); de naam van de aanvrager van een tool; teksten in het AI-beleid; naam, categorieën en niveaus van eigen programma's; geletterdheidsgegevens: toegewezen e-learnings, "afgerond" met datum, niveau (geen score; Staff heeft er geen leesrechten op zonder zichzelf eerst toe te voegen als lid van de workspace, artikel 3.2)
Bijzondere persoonsgegevens	Niet bedoeld. De AUP verbiedt ze in te voeren. Verwerker kan niet uitsluiten dat de klant ze in vrije tekst invoert
Duur	De looptijd van de Hoofdovereenkomst plus de termijnen uit artikel 10. Gesprekken met de AI-assistent: zolang de workspace bestaat, tenzij de Gebruiker ze eerder verwijdt (Bijlage 4, artikel 4.9). Organisationsprofiel: zolang de workspace bestaat. Persoonlijke instructies: tot de Gebruiker ze wist of het lidmaatschap eindigt

Locatie	Klantgegevens worden opgeslagen in de EU (Frankfurt). Verwerking en toegang van buiten de EER vinden plaats voor ondersteunende functies, onder de waarborgen in Bijlage 3 (artikel 5.4). AI-verwerking vindt plaats in de EU (Bijlage 4). Een eigen AI-koppeling van de Klant: alleen naar een Europees eindpunt van de aanbieder (Bijlage 4, artikel 4.23). Verwerker belooft niet dat de aanbieder uitsluitend in de EU verwerkt (artikel 4.24)
Eigen doeleinden van Verwerker (Verwerker is daarvoor verantwoordelijke)	(a) de eigen klantrelatie en facturatie, waaronder de Bedrijfsgegevens van de Klant (zoals gedefinieerd in de Algemene Voorwaarden, artikel 1.2) en de gegevens die nodig zijn om te factureren (naam, factuuradres, e-mailadres voor facturen), de prijsbevestiging (wie, wanneer), kortingen en de platformfee (verwijzing naar de afgeronde Opdracht, bedrag, datum). Verwerker gebruikt Exact als zijn eigen verwerker voor de facturatie. Er gaan geen Klantgegevens, geen gegevens van individuele Gebruikers en geen workspace-inhoud naar Exact. Het gaat om wat op een factuur staat: bedrijfsnaam, factuuradres, btw-id, e-mailadres voor facturen en de naam van een contactpersoon. De factuur noemt de Partner en de Reactie niet. Wat op een factuur en in de financiële administratie van Verwerker staat, bewaart Verwerker 7 jaar na afloop van het boekjaar (art. 52 lid 4 AWR en art. 2:10 BW), waaronder het bewijs van de btw-behandeling (btw-id en VIES-bewijs), ook als de Hoofdovereenkomst eindigt. De overige Bedrijfsgegevens, ook hun wijzigingshistorie (artikel 10.3), verwijdt Verwerker uiterlijk 30 dagen na het einde van de Hoofdovereenkomst; (b) de bewaring van gepseudonimiseerde audit-gebeurtenismetadata na het einde van de Hoofdovereenkomst, voor rechtsvorderingen (artikel 10.3); (c) het bewijs van acceptatie van deze VWO en de Hoofdovereenkomst (versie, hash, tijdstip, bevoegdheidsverklaring) en van de verklaring over de EU en het zakelijk handelen (tekstversie, tijdstip), looptijd plus 5 jaar (Privacyverklaring).

Bijlage 2

Technische en organisatorische maatregelen

1. Datalocatie.

- Klantgegevens staan in Frankfurt (Supabase, eu-central-1): database en authenticatie.
- De applicatiefuncties draaien in Frankfurt (Vercel, fra1). Verkeer loopt via het wereldwijde netwerk van Vercel. Vercel kan verwerking uitvoeren in de VS en elders. Daarvoor gelden SCC's en het DPF (Bijlage 3).
- Voor inzage- en verwijderverzoeken over chatinhoud draait een procedure bij GitHub (VS). De uitvoer is versleuteld en staat maximaal één dag bij GitHub. De sleutel staat niet bij GitHub (Bijlage 3, artikel 7).
- Monitoring zonder persoonsgegevens draait op door GitHub gehoste runners. De uitrol van Edge Functions en het beheer van de Vercel-configuratie doet Verwerker lokaal, niet via GitHub; het Supabase- en het Vercel-token zijn uit GitHub verwijderd en ingetrokken (Bijlage 3).
- CI controleert de regio's (`scripts/check-regions.sh`, `check-supabase-region.sh`, `check-supabase-branch-regions.sh`). Dit geldt niet voor GitHub-runners.
- AI-verwerking (alleen als de Admin dit inschakelt) draait via AWS in regio's binnen de EU (Deel A) of via een Europees eindpunt van de eigen aanbieder van de Klant (Deel B; Bijlage 3 en 4).

2. Scheiding tussen klanten. Row Level Security in PostgreSQL op elke tabel met klantdata, gekoppeld aan het lidmaatschap van de gebruiker. Een CI-controle (`db/checks/rls_guard.sql`) laat de build falen als een policy ontbreekt.

3. Least privilege. Een aparte databaserol per domeinmodule en geen gedeelde superuser. Wijzigingen lopen via gecontroleerde databasefuncties.

4. Versleuteling.

- TLS voor al het verkeer.
- Versleuteling at rest door Supabase.
- Aanvullende versleuteling op applicatieniveau voor de uitvoer van de procedure voor chatinhoud (artikel 7); de sleutel staat niet bij GitHub.
- Sleutels van eigen AI-koppelingen staan in Supabase Vault. Het Platform bewaart alleen de laatste vier tekens. Een sleutel gaat nooit naar de browser, logs of de audit-trail.

5. Secrets. Geen secrets in de broncode; een secret-store met rotatiebeleid.

6. Logging en audit.

- Elke businessmutatie schrijft een onveranderlijk `AuditEvent` (append-only, technisch afgedwongen): wie, wanneer, wat.
- Via het Platform legt Verwerker per staff-lid per workspace één gebeurtenis per 30 minuten vast (`staff_workspace_accessed`), met een reden uit een vaste lijst. Dat geldt voor workspaces waarvan de medewerker geen lid is.
- Zet de Admin proactieve begeleiding uit (`proactive_guidance_enabled_changed`), dan weigert het Platform de reden "monitoring en begeleiding". Dit is een organisatorische maatregel. Staff kan technisch alle workspace-inhoud lezen, behalve chatinhoud, persoonlijke instructies en geletterdheidsgegevens per persoon. Verwerker controleert de gekozen redenen wanneer er een vermoeden of aanleiding voor is. Support, incident en adviesopdracht blijven mogelijk; adviesopdracht alleen bij een lopende offerte of opdracht (artikel 3.2).

- Voor chatthreads legt het Platform alleen workspace, aanmaker, tijdstip en aantal deelnemers vast, niet de inhoud (artikel 3.3).
- Handmatige toegang tot Klantgegevens buiten het Platform legt Verwerker vast in een logboek (artikel 3.4).
- Voor AI-gesprekken legt het Platform alleen workspace, aanmaker en soort vast (thread_created), wijzigingen aan de AI-instelling en eigen koppelingen (ai_provider_config_changed, zonder sleutel, hint of host), wijzigingen aan het organisatieprofiel met hash en lengte (ai_workspace_profile_changed) en dat persoonlijke instructies zijn opgeslagen of gewist (ai_user_instructions_changed), nooit de inhoud.

7. Toegangsbeheer.

- Inloggen via een magic link of bevestigingslink, verzonden via de transactionele e-maildienst (Bijlage 3), of via een identiteitsprovider (Microsoft Entra ID of Google; zie Bijlage 3, "Identiteitsproviders"). De link bevat een eenmalig token met een korte geldigheidsduur. De e-mail toont geen inhoudspreview van de workspace. Bij inloggen met een link ontstaat een account pas na bevestiging van de mailbox. Een inlogroute geeft zelf geen toegang tot een Workspace. Toegang volgt uit het lidmaatschap, dat de Admin beheert. Een lidmaatschap ontstaat pas nadat Verwerker de mailbox van het betreffende adres met een eigen bevestigingsmail heeft bevestigd; een bevestiging door een identiteitsprovider geldt daarvoor niet. Beëindigt een Admin een lidmaatschap, dan vervalt de toegang, ongeacht de gebruikte inlogroute.
- Rollen: admin en member.
- Een Partner heeft na een Keuze alleen toegang tot dat ene project. De afscherming is Row Level Security per project. Een test toont dat een Partner niets ziet van een niet-gekoppelde Klant.
- Staff heeft via het Platform toegang tot workspaces, behalve tot chatinhoud en persoonlijke instructies (artikel 3.3 en Bijlage 4, artikel 4.16). Die toegang vraagt een reden. Het Platform logt die per staff-lid per workspace één keer per 30 minuten (punt 6).
- Staff heeft geen leesrechten op geletterdheidsgegevens zonder zichzelf eerst toe te voegen als lid van de workspace; dat toevoegen zelf wordt vastgelegd en gemeld aan de Admin (artikel 3.2). Technisch: Row Level Security zonder uitzondering voor staff; het toevoegen, ook met de rol Admin, wordt vastgelegd als membership_added (bron staff) en verschijnt als melding bij de Admin.
- Externe toegang staat technisch dicht tot een platformbrede poort bewust opengaat.

8. Openbare routes.

- Rate limiting en misbruikdetectie.
- Zelf-gehoste captcha (ALTCHA): geen extern captcha-netwerk, geen gegevensdeling met een derde partij.
- Persoonlijke links hebben minstens 128 bits toeval, staan alleen als hash opgeslagen, verlopen na maximaal 90 dagen, zijn intrekbaar en staan op noindex.

9. Ontwikkelproces.

- Review van elke wijziging, inclusief een security-review.
- Dependency scanning en SBOM.
- Databasemigraties alleen geautomatiseerd, nooit met de hand: voor de test- en acceptatieomgeving via de Supabase-GitHub-koppeling, voor productie zoals hieronder.
- Productiemigraties lopen via de Supabase-GitHub-koppeling in Frankfurt. Het databasewachtwoord (SUPABASE_DB_PASSWORD) is na de omzetting uit GitHub verwijderd en geroteerd.

10. **Testen.** Een interne security-test volgens OWASP ASVS 5.0 niveau 2 vóór externe toegang, op een acceptatieomgeving met synthetische data. Verwerker lost kritieke en hoge bevindingen op vóór de ingebruikname. Een onafhankelijke pentest volgt zodra een klant, verzekeraar of aanbesteding erom vraagt, en vóór de eerste grotere klant.
11. **Back-ups en continuïteit.** Supabase maakt dagelijks een back-up, los van de projectopslag, versleuteld met AES-256 in rust; transport loopt via TLS. Back-ups worden 7 dagen bewaard. Er is geen point-in-time-herstel. De back-ups maakt en bewaart Supabase volgens zijn eigen inrichting voor het project (zie Bijlage 3).
12. **Incidentrespons.**
 - Contactpunt van Verwerker voor incidenten: info@norwin.ai.
 - Verwerker meldt een inbreuk zonder onredelijke vertraging en streeft ernaar dat binnen 48 uur te doen (artikel 8.1).
 - Verwerker handelt incidenten af volgens een vastgestelde interne procedure.

Bijlage 3

Subverwerkers

Subverwerker	Entiteit en vestiging	Dienst	Locatie van de data	Doorgifte en waarborg
Supabase	Supabase Pte. Ltd., 65 Chulia Street #38-02/03, OCBC Centre, Singapore 049513 (moeder: Supabase Inc., VS). Supabase DPA versie 1, 1 augustus 2026	Database, authenticatie, opslag van sleutels van eigen AI-koppelingen (Supabase Vault)	Frankfurt, Duitsland (EU), de regio die Verwerker zelf koos (Supabase DPA art. 6.1). Daar staat de data en vindt de verwerking in de eerste plaats plaats	Singapore heeft geen adequaatheidsbesluit. Voor Singapore gelden SCC's module 3 (verwerker naar subverwerker), onder lers recht met de Ierse rechter (Supabase DPA art. 12, Schedule 2). Doorgiftetoets. Supabase Pte. Ltd. (Singapore) is contractpartij; moeder: Supabase Inc. (VS). De gegevens staan in Frankfurt (eu-central-1), versleuteld in rust. Supabase staat niet op de DPF-lijst (gecontroleerd 2026-10-10 op dataprivacyframework.gov). De doorgifte rust op de SCC's (module 3) uit de Supabase-DPA, onder lers recht. Support en operations werken wereldwijd; toegang van buiten de EER is mogelijk en wordt gelogd. Norwin beoordeelt deze doorgifte voorlopig en herbeoordeelt haar binnen 12 maanden. Het verkeer loopt via TLS en Row Level Security scheidt klanten onderling. Supabase meldt een wijziging in zijn subverwerkers 30 dagen vooraf aan wie zich aanmeldde, met een bezwaartermijn van 5 dagen (https://supabase.com/legal/customer-resources/subprocessor-list). Verwerker is voor die meldingen aangemeld en geeft ze door volgens artikel 5.2. Supabase meldt een datalek zonder onredelijke vertraging, waar mogelijk binnen 48 uur. Verwijdering binnen 30 dagen na het einde. Afwijkingen van deze VVO (artikel 5.3): bezwaartermijn bij een nieuwe subverwerker 5 dagen in plaats van 30 (opgevangen door artikel 5.2); datalekmelding "waar mogelijk binnen 48 uur", geen harde termijn.

Vercel	Vercel Inc. (Delaware, VS). Vercel DPA versie 17 maart 2026, van kracht vanaf 31 maart 2026. De DPA geldt via het Pro-plan; Verwerker gebruikt het Pro-plan, met Vercel Inc. als contractpartij.	Hosting en uitvoering van de applicatie	Klantgegevens worden opgeslagen in Frankfurt (Supabase). De applicatiefuncties draaien in Frankfurt. Verkeer loopt via het wereldwijde netwerk van Vercel, en Vercel kan verwerking uitvoeren in de VS en elders. Daarvoor gelden SCC's en het DPF. Gebruiksdata zoals IP-adressen in logs verwerkt Vercel deels als zelfstandig verantwoordelijke, onder zijn eigen privacyverklaring	Vercel Inc. is gecertificeerd onder het DPF. SCC's (module 3) gelden als terugval, onder lers recht, met de Ierse gegevensbeschermingsautoriteit (DPC) als toezichthouder. Voor gebruiksdata als zelfstandig verantwoordelijke zie Vercel DPA art. 4.b. Vercel meldt zijn subverwerkers alleen aan wie zich per e-mail aanmeldde bij privacy@vercel.com , met een bezwaartermijn van 5 dagen. Verwerker geeft die melding door volgens artikel 5.2. Verwerker heeft de aanmelding voor subverwerkersmeldingen aangevraagd via privacy@vercel.com (oktober 2026). Vercel meldt een datalek zonder onredelijke vertraging, zonder vaste termijn in uren. Afwijkingen van deze VWO (artikel 5.3): datalekmelding zonder termijn in uren; bezwaartermijn bij een nieuwe subverwerker 5 dagen in plaats van 30 (opgevangen door artikel 5.2). Vervalt het DPF, dan geldt artikel 6.3
---------------	--	---	--	--

Brevo (Sendinblue SAS)	Sendinblue SAS, Parijs (RCS 498 019 298). Frans recht is van toepassing op de DPA. Het Tribunal de commerce te Parijs is bevoegd. Alleen de Engelse tekst van de DPA is bindend. Verwerker gebruikt het gratis plan (Free) van Brevo; contractpartij is Sendinblue SAS (Brevo), Parijs (EU).	Transactionele e-mail: inlog-, bevestigings-, uitnodigings- en documentmails (ook de PDF's van de geaccepteerde documenten, Algemene Voorwaarden art. 2.4). Brevo is de enige mailsubverwerker. De ingebouwde mailer van Supabase is niet in gebruik	Opslag in de EU: OVH (Frankrijk en Duitsland) en Google Cloud (België)	Brevo's subverwerkerslijst noemt partijen met toegang van buiten de EER: Cloudflare (VS/EU) en Zendesk (support, EU/VS) voor infrastructuur en support, en de groepsentiteiten Brevo CRM Solutions (India) en Sendinblue Inc. (VS) voor klantenservice en onderhoud. Mechanisme: DPF of SCC's voor de VS; SCC's voor India (geen adequaatheidsbesluit). Actuele lijst: Annex 2 bij de DPA van Brevo (Appendix 3 bij de Brevo Terms, versie 1 oktober 2025). Verwerker stuurt via Brevo geen workspace-inhoud, alleen e-mailadres, naam en een link. De inhoudspreview staat uit. Verwerker heeft klik- en opentracking in het Brevo-account uitgezet voor de transactionele mail van het Platform, voor zover Brevo dat toelaat. Dat geldt ook voor de inlog- en bevestigingsmail die het Platform via de SMTP-relay of de transactional API van Brevo verstuurt. Brevo mag gebruiksdata (niet: Klantgegevens of workspace-inhoud) gebruiken voor eigen fraude- en spampreventie (Brevo ToS art. 6.7). Dat is geen training van een generatief AI-model op Klantgegevens. Brevo meldt een nieuwe subverwerker zonder vaste minimumtermijn en een datalek "without undue delay", zonder uren-termijn. Voor de nieuwe subverwerker geldt artikel 5.2, tweede deel. Afwijkingen van deze VWO (artikel 5.3): datalek melding zonder termijn in uren; geen vaste minimumtermijn voor de melding van een nieuwe subverwerker
---------------------------------------	--	--	--	---

GitHub	GitHub, Inc., 88 Colin P. Kelly Jr. Street, San Francisco, California 94107, VS. GitHub Data Protection Agreement, "Version: October 2025". GitHub beschikt over SOC 1- en SOC 2 Type 2-rapporten en een ISO 27001-certificering.	(a) Uitvoeren van de gelogde procedure voor inzage- en verwijderverzoeken over chatinhoud (artikel 7), alleen bij een schriftelijk verzoek of een incident. (b) Monitoring zonder persoonsgegevens: de opruimwachtrij en de uptimecheck van de publieke /api/health (antwoord zonder persoonsgegevens: een statuscode en een vaste statuswaarde, ok, degraded of rate_limited). De geplande controle van de opruimwachtrij voor profielfoto's en bedrijfslogo's ziet alleen de URL van de opruimtaak, een statuscode en drie getallen (aantal, leeftijd van de oudste rij, regio); geen persoonsgegevens en geen Klantgegevens. Zie de voorwaarden onder deze tabel. Credential: STORAGE_REMOVALS_STATUS_TOKEN, dat alleen die status kan opvragen en niets kan starten; geen toegang tot Klantgegevens. Een eerder doel (c), CI/CD met een Supabase- en een Vercel-token, is vervallen (zie onder de tabel)	VS (volgens GitHub's subverwerkerslijst hostet Microsoft Azure in de VS). Voor doel (a) staat bij GitHub één versleuteld bestand, dat na één dag verloopt (retention-days: 1), en de metadata van de uitvoering: workspace-ID, ID van de betrokkene, dossiernummer, reden, het staff-ID van de uitvoerder (operator_user_id) en de GitHub-login van degene die de procedure start. De job summary toont het aantal geredigeerde berichten. Nooit chatinhoud in leesbare vorm. De sleutel voor ontsleuteling staat niet bij GitHub. De verbindingsgegevens voor de database (CHAT_DSR_DATABASE_URL, databaserol chat_dsr_runner met minimale rechten) staan als omgevingsgeheim bij GitHub. De runner in de VS verbindt met de database in Frankfurt; daar komt alleen ciphertext uit terug. Run-metadata en logs blijven 90 dagen bewaard (de standaardinstelling); Verwerker kan die termijn verlagen.	GitHub, Inc. is zelf in de VS gevestigd. De doorgifte steunt op GitHub's zelfcertificering onder het DPF en/of de SCC's (GitHub DPA 7.B). Van de SCC's geldt Module Two of Three, naar gelang de rol; voor Verwerker als verwerker is dat Module Three (verwerker naar subverwerker), onder Nederlands recht met de Nederlandse rechter (DPA 7.C.ii). Annex IV van de DPA geeft aanvullende waarborgen: GitHub vecht verzoeken van overheden aan, informeert de klant daarover, en vergoedt schade van betrokkenen. Toegang op grond van Amerikaans recht is niet uitgesloten. GitHub meldt nieuwe subverwerkers 30 dagen vooraf aan wie zich aanmeldt via https://gh.io/subscribe (DPA 9.B); bij bezwaar kan de klant van GitHub kosteloos opzeggen (DPA 9.C). Actuele lijst: https://github.com/github-subprocessors-list. Verwerker is daarvoor aangemeld en geeft die melding door volgens artikel 5.2. GitHub meldt een Security Incident "without undue delay" (DPA 6.A), zonder termijn in uren. Afwijkingen van deze VWO (artikel 5.3): datalek melding zonder termijn in uren. Vervalt het DPF, dan geldt artikel 6.3
---------------	--	---	--	---

Amazon Web Services (Amazon Bedrock)	Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxemburg (moeder: Amazon Web Services, Inc. / Amazon.com, Inc., VS). AWS GDPR Data Processing Addendum, versie 14 augustus 2026, onderdeel van de AWS Service Terms	Alleen voor de Module AI-verwerking (Bijlage 4, Deel A), alleen voor workspaces waarvan de Admin chat met AI inschakelt: het draaien van het AI-model van Bijlage 4, artikel 4.4 (de actuele modelnaam staat op de pagina "Datalocatie en toegang door overheden", https://app.norwin.ai/datalocatie) voor de AI-chat, met de context uit Bijlage 4, artikel 4.15 tot en met 4.17	Aanvragen gaan vanuit Frankfurt (eu-central-1) via een Europees inferentieprofiel; AWS kan ze binnen de EU naar een andere AWS-regio sturen. Geen regio buiten de EU. Verwerker gebruikt alleen modellen met retentiemodus "none"; voor misbruikdetectie zie Bijlage 4, artikel 4.8	AWS EMEA SARL zit in de EU. Amazon.com, Inc. is gecertificeerd onder het EU-VS Data Privacy Framework (DPF), met Amazon Web Services, Inc. als gedekte entiteit (gecontroleerd op 5 oktober 2026 op dataprivacyframework.gov ; volgende hercertificering uiterlijk 2 januari 2027); de SCC's zitten in de AWS-DPA (module 3 voor Verwerker als verwerker). Het moederbedrijf is Amerikaans: toegang op grond van Amerikaans recht (CLOUD Act, FISA 702) is niet uitgesloten, ook bij verwerking in de EU. Toegang door AWS-personeel alleen om de dienst te leveren of om aan de wet te voldoen (AWS Customer Agreement, artikel 1.4). AWS meldt nieuwe subverwerkers minstens 30 dagen vooraf via https://aws.amazon.com/compliance/sub-processors/ aan wie zich aanmeldt. Verwerker is daarvoor aangemeld (4 oktober 2026) en geeft de melding door volgens artikel 5.2. AWS' bezwaarmogelijkheid: de overeenkomst beëindigen, de dienst niet meer gebruiken of de data naar een andere regio verplaatsen. Afwijkingen van deze VWO (artikel 5.3): datalek melding zonder termijn in uren: AWS meldt een Security Incident zonder onredelijke vertraging (AWS DPA, artikel 9.1; Bijlage 4, artikel 4.13); AWS kent geen bezwaarprocedure voor een nieuwe subverwerker, alleen de mogelijkheden hierboven (de overeenkomst beëindigen, de dienst niet meer gebruiken of de data naar een andere regio verplaatsen), opgevangen door artikel 5.2. Vervalt het DPF, dan geldt artikel 6.3
---	---	--	---	---

Partners zijn geen Subverwerker. Een Partner die via een Keuze toegang krijgt tot een project van de Verwerkingsverantwoordelijke, is geen Subverwerker van Verwerker (artikel 3.5).

Exact (geen Subverwerker). Exact staat bewust niet in deze tabel: Verwerker gebruikt Exact als eigen verwerker voor de facturatie (Bijlage 1, eigen doeleinden). Gaan er persoonsgegevens van Gebruikers of workspace-inhoud naar Exact, dan wordt Exact een Subverwerker en komt het in deze tabel.

GitHub, doel (b): voorwaarden. De uptimecheck vraagt alleen de publieke statuspagina van het Platform op. Die geeft alleen een statuscode (200, 503 of bij te veel verzoeken 429) met een vaste statuswaarde (ok, degraded of rate_limited), en nooit persoonsgegevens, Klantgegevens, namen, kenmerken of foutmeldingen. Een storingsmelding gaat naar het eigen meldkanaal van Verwerker (Slack) en wordt gebouwd uit een vaste template van vijf velden: omgeving, vaste naam van de controle, status (ok of rood), tijdstip en een link naar de run. Er is geen vrij tekstveld. In dit bericht staan geen persoonsgegevens of Klantgegevens. Een nieuw veld of een nieuwe controle met meer dan een vaste naam toetst Verwerker eerst opnieuw.

Anthropic Ireland, Limited levert het model, maar ontvangt volgens AWS geen Klantgegevens. Anthropic is geen Subverwerker van Verwerker (Bijlage 4, artikel 4.4). **GitHub, vervallen doel (c): CI/CD-workflows.** De workflows voor de uitrol van Edge Functions (`edge-functions.yml`), de controles van configuratie en beveiligingsadviezen (`supabase-drift.yml`; job advisors in `ci.yml`) en het beheer van de Vercel-configuratie (`vercel-env.yml`) draaiden op door GitHub gehoste runners, met een accountbreed Supabase-token en een teambreed Vercel-token:

- **Verwijderd.** Deze workflows en het Supabase- en Vercel-token zijn uit GitHub verwijderd en de tokens zijn ingetrokken. De uitrol van Edge Functions, de controles en het beheer van de Vercel-configuratie doet Verwerker lokaal, niet via GitHub. Doel (c) is vervallen.
- **Productiemigraties** lopen via de Supabase-GitHub-koppeling in Frankfurt. Het databasewachtwoord (SUPABASE_DB_PASSWORD) is na de omzetting uit GitHub verwijderd en geroteerd.
- **Wat in GitHub blijft.** In GitHub staat geen secret met toegang tot Klantgegevens of tot de hosting (Supabase, Vercel), op één uitzondering na: CHAT_DSR_DATABASE_URL voor doel (a), een databaselogin met minimale rechten (rol chat_dsr_runner) waarmee alleen versleutelde uitvoer terugkomt. Verder blijven alleen secrets zonder zo'n toegang, zoals STORAGE_REMOVALS_STATUS_TOKEN voor doel (b) (alleen aantallen, leeftijd en regio), SLACK_ALERT_WEBHOOK_URL (alleen om de vaste melding van vijf velden te versturen), de publieke sleutel voor de versleuteling van doel (a) en tokens voor het bijhouden van het projectbord.

Identiteitsproviders (geen Subverwerkers). Een Gebruiker kan zich aanmelden en inloggen met een Microsoft-werk- of schoolaccount (Entra ID) of met een Google-account, naast de e-maillink; de Gebruiker kiest dat zelf. Microsoft en Google zijn daarbij zelf verantwoordelijk voor het inloggen bij het eigen account van de Gebruiker, of handelen als verwerker van de organisatie die dat account beheert, bijvoorbeeld de werkgever. In beide gevallen is Verwerker niet hun opdrachtgever: Verwerker schakelt hen niet in om Klantgegevens te verwerken en geeft hen geen instructies; zij zijn daarom geen Subverwerker. Verwerker ontvangt van de provider onder meer het e-mailadres, de naam, de vaste account-ID bij de provider en, bij Microsoft, de tenant-ID. Verwerker slaat alleen op: de naam van de provider, de vaste account-ID van de Gebruiker bij de provider, het e-mailadres, de naam en, bij Microsoft, het ID van de organisatie (tenant). Andere gegevens die de provider meestuurt, bewaart Verwerker niet. Verwerker vraagt alleen die scopes, neemt de profielfoto van de provider niet over, bewaart geen toegangs- of verversingstoken van de provider en geeft geen Klantgegevens aan de provider. Verwerker slaat de ontvangen identiteitsgegevens op bij Supabase (Frankfurt, zie hierboven). De provider verwerkt zelf op locaties die Verwerker niet bepaalt, ook buiten de EER; Verwerker garandeert geen verwerking uitsluitend in de EU door de provider.

Door de Klant gekozen AI-aanbieders zijn geen Subverwerkers: zie Bijlage 4, artikel 4.21.

Subverwerkerslijst van Norwin: de pagina "Datalocatie en toegang door overheden" (/datalocatie in het Platform), samen met deze Bijlage 3.

Bijlage 4

Module AI-verwerking

Deze module heeft twee delen. Deel A (artikel 4.1 tot en met 4.18) gaat over chat met de AI van Verwerker, via Amazon Bedrock. Deel B (artikel 4.20 tot en met 4.29) gaat over een eigen AI-koppeling die de Admin zelf toevoegt. Een workspace kan beide gebruiken. De Gebruiker kiest per gesprek welke.

Deel A

AI van Verwerker

- 4.1 **Werking.** Deze module geldt voor een workspace vanaf het moment dat de Admin chat met AI inschakelt en deze module (versie 1.2 of hoger) accepteert. Zolang de functie uit staat (de standaard) of de module niet is geaccepteerd, stuurt Verwerker geen Klantgegevens naar een AI-dienst, ook niet naar een eigen AI-koppeling van de Klant. Het Platform weigert de functie dan. Deze module geldt niet voor chat tussen collega's; die gebruikt geen AI. Met de acceptatie van deze module geeft Verwerkingsverantwoordelijke de instructie voor de verwerking die in de artikelen 4.2, 4.3 en 4.15 tot en met 4.18 en in Bijlage 1 is beschreven (artikel 28 lid 3 onder a AVG).
- 4.2 **Doel.** Gebruikers van de workspace kunnen in het Platform een gesprek voeren met een AI-assistent en krijgen daarop gegenereerde antwoorden. Zij kunnen daarbij het organisatieprofiel, hun persoonlijke instructies en kansen en projecten van hun workspace als context laten meegaan (artikel 4.15 tot en met 4.17) en voorstellen krijgen voor een kans of taak (artikel 4.18). Verwerker verwerkt de gegevens uitsluitend om dat mogelijk te maken (artikel 2.1 van de Verwerkersovereenkomst). Wat een Gebruiker invoert, is aan Verwerkingsverantwoordelijke en zijn Gebruikers.
- 4.3 **Wat er verwerkt wordt.**
- De invoer die een Gebruiker in het gesprek geeft en de eerdere berichten van hetzelfde gesprek (maximaal 40 berichten per aanroep).
 - De gegenereerde antwoorden.
 - Het organisatieprofiel (artikel 4.15), de persoonlijke instructies van de Gebruiker (artikel 4.16) en, als de Gebruiker dat voor het gesprek kiest, kansen en projecten (artikel 4.17).
 - Het Platform stuurt geen andere gegevens uit de workspace mee. Wil Verwerker dat wel doen, dan volgt hij artikel 4.11.
 - Een Gebruiker kan in een gesprek elk soort gegeven invoeren, ook over derden. Bijzondere persoonsgegevens zijn niet bedoeld (artikel 4.10).
 - De audit-trail legt vast dat een gesprek is gemaakt, wijzigingen aan de AI-instelling, en wijzigingen aan het organisatieprofiel (alleen hash en lengte) en aan persoonlijke instructies (alleen dát ze zijn opgeslagen of gewist). Nooit de inhoud van een gesprek, een profiel of een instructie.
- 4.4 **Subverwerker en model.** Verwerker gebruikt voor Deel A één Subverwerker: Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxemburg, via Amazon Bedrock (Bijlage 3). AWS laat het model draaien en is de operator.
- Het AI-model is een model van Anthropic, gebruikt via AWS Bedrock in de EER. De actuele modelnaam staat op <https://app.norwin.ai/datalocatie>. Een wijziging van het model kondigt Norwin AI 30 dagen vooraf aan. De regio's staan in artikel 4.5. Een wijziging van het model volgt artikel 4.8, 4.11 en 4.12 van deze Bijlage en artikel 5.2 van de Verwerkersovereenkomst.
 -

AWS draait het model in een Model Deployment Account dat AWS beheert. Anthropic heeft geen toegang tot dat account, en AWS deelt invoer en uitvoer niet met Anthropic (documentatie van Amazon Bedrock, "Data protection", <https://docs.aws.amazon.com/bedrock/latest/userguide/data-protection.html>, geraadpleegd op 5 oktober 2026). Anthropic verwerkt daardoor geen persoonsgegevens namens Verwerker en is geen Subverwerker van Verwerker.

- Verwerker gebruikt het model onder de Anthropic on Bedrock Commercial Terms (versie 18 augustus 2025), met Anthropic Ireland, Limited als contractpartij van Verwerker. De verwerkersovereenkomst van Anthropic maakt daar door verwijzing deel van uit. Die geldt als vangnet: krijgt Anthropic ooit toch toegang tot invoer of uitvoer, dan is Anthropic een nieuwe Subverwerker en geldt artikel 5.2 van de Verwerkersovereenkomst.
- Verwerker gebruikt de directe API van Anthropic niet.
- Het model krijgt geen hulpmiddelen: het kan niets opzoeken, aanroepen of uitvoeren, en kan niets in het Platform wijzigen. Het ziet het gesprek en de context die artikel 4.3 noemt, en niets anders. Het Platform stuurt alleen tekst naar het model.

4.5 **Locatie.** Verwerker laat het model uitsluitend draaien via een Europees inferentieprofiel van AWS. Aanvragen gaan vanuit Frankfurt en AWS kan ze binnen de EU sturen naar Frankfurt, Stockholm, Milaan, Spanje, Ierland of Parijs (voor beide modellen vastgesteld via Amazon Bedrock op 5 oktober 2026). Verwerker gebruikt geen profielen of regio's buiten de EU.

4.6 **Doorgifte en overheden buiten de EU.** AWS EMEA SARL is gevestigd in de EU. Het concern waartoe AWS behoort, Amazon.com, Inc., is Amerikaans. Op grond van Amerikaans recht (zoals de CLOUD Act en FISA 702) kan een Amerikaanse instantie toegang vorderen, ook als de verwerking in de EU plaatsvindt.

- Vraagt een overheid AWS om Klantgegevens, dan probeert AWS de instantie door te verwijzen naar Verwerker en informeert AWS Verwerker vooraf, tenzij dat wettelijk verboden is (AWS DPA, artikel 3).
- AWS-ondersteuning verwerkt Klantgegevens alleen als Verwerker die zelf deelt in een supportverzoek. Verwerker deelt geen inhoud van gesprekken met AWS-ondersteuning.
- Voor doorgifte buiten de EER gelden de standaardcontractbepalingen in de AWS DPA en de DPF-certificering van AWS (Bijlage 3). Vervalt het DPF, dan geldt artikel 6.3 van de Verwerkersovereenkomst.
- Met acceptatie van deze module bevestigt Verwerkingsverantwoordelijke kennis te hebben genomen van deze beschrijving en daarmee akkoord te gaan.

4.7 **Geen training.** Verwerker gebruikt invoer en uitvoer niet om modellen te trainen. AWS doet dat volgens zijn documentatie niet (Amazon Bedrock, "Data protection"), en Anthropic mag dat volgens zijn voorwaarden niet. Dit sluit aan bij artikel 2.5 van de Verwerkersovereenkomst en artikel 9 van de Algemene Voorwaarden. Voor Deel B zie artikel 4.28.

4.8 **Bewaring bij AWS.**

- Verwerker schakelt het loggen van volledige aanvragen en antwoorden (model invocation logging) in zijn AWS-account niet in.
- Behalve zoals hieronder beschreven, stelt Verwerker de retentiemodus "none" in, voor elke AWS-regio van waaruit het Platform het model aanroept. Volgens de documentatie van AWS geldt de retentiemodus voor elk verzoek in de regio waar hij is ingesteld. Streaming wordt in die documentatie niet apart genoemd. Onder die modus schrijft AWS geen aanvraag- of

antwoordgegevens naar duurzame opslag en deelt AWS ze niet met de modelaanbieder. Verwerker gebruikt geen model dat bewaring of beoordeling door AWS of de modelaanbieder vereist, of waarvoor AWS gegevens met de modelaanbieder deelt.

- Volgens de documentatie van AWS kan AWS bij vermoedelijk beeldmateriaal van seksueel kindermisbruik in afbeeldingen de gemarkeerde invoer of uitvoer opslaan en beoordelen om dat vast te stellen, en melden bij de bevoegde instantie (documentatie van Amazon Bedrock, "Amazon Bedrock abuse detection", <https://docs.aws.amazon.com/bedrock/latest/userguide/abuse-detection.html>, geraadpleegd op 5 oktober 2026). Het Platform stuurt alleen tekst. AWS kan daarnaast gegevens bewaren of verstrekken als een wettelijke verplichting dat vereist (artikel 4.6). Met acceptatie van deze module bevestigt Verwerkingsverantwoordelijke deze beschrijving te kennen.
- Het Platform kan een antwoord als stroom ontvangen (streaming), zodat de Gebruiker het tijdens het genereren leest. Daarvoor gelden hetzelfde model en hetzelfde Europese inferentieprofiel. Het Platform slaat een afgebroken stroom niet op (artikel 4.9).
- Verandert dit voor een gebruikt model, dan volgt Verwerker de procedure van artikel 4.11 voordat hij het model nog gebruikt.

4.9 **Bewaring in het Platform.**

- Een gesprek is persoonlijk. Alleen de Gebruiker die het voerde kan het in het Platform lezen. Andere Gebruikers, ook de Admin, en Staff van Verwerker kunnen dat niet. Voor Staff geldt artikel 3.3 van de Verwerkersovereenkomst op dezelfde manier als bij chat tussen collega's, met de uitzonderingen van artikel 3.4 en 7.
- Heeft Verwerkingsverantwoordelijke een concrete aanleiding, zoals misbruik, een datalek of een rechtsvordering, dan kan hij Verwerker schriftelijk vragen een bepaald gesprek te lezen of te verwijderen volgens artikel 3.4 en 7. Verwerkingsverantwoordelijke is zelf verantwoordelijk voor een grondslag en voor de informatie aan zijn medewerkers.
- Verwerker bewaart gesprekken zolang de workspace bestaat, zodat de Gebruiker zijn eerdere gesprekken kan terugvinden.
- De Gebruiker kan zijn eigen gesprek verwijderen. Uit back-ups verdwijnt het binnen de termijn van Bijlage 2, punt 11 (7 dagen).
- Een verzoek van een betrokkene verloopt volgens artikel 7 van de Verwerkersovereenkomst. Bij het einde van de Hoofdovereenkomst gelden de termijnen van artikel 10.
- Een antwoord kan gegevens uit de context bevatten. Die blijven met het gesprek bewaard, ook als het project later wijzigt of wordt verwijderd, tot de Gebruiker het gesprek verwijdert of de workspace eindigt.
- Het Platform slaat een afgebroken antwoord niet op.
- Het organisatieprofiel en de persoonlijke instructies zijn geen gesprekken. Voor hen gelden artikel 4.15 en 4.16.

4.10 **Verplichtingen van de Verwerkingsverantwoordelijke.**

- Hij voert zelf geen bijzondere persoonsgegevens in en instrueert zijn Gebruikers dat niet te doen (AUP). Verwerker kan niet uitsluiten dat dit toch gebeurt.
- Hij is verantwoordelijk voor een grondslag voor wat zijn Gebruikers invoeren en voor transparantie richting zijn medewerkers.
- Hij informeert zijn medewerkers dat zij met een AI-systeem werken. Het Platform maakt in de chat duidelijk dat het antwoord van een AI komt en dat het onjuist of onvolledig kan zijn.

- Hij informeert zijn Gebruikers dat het organisatieprofiel bij elk gesprek van elke Gebruiker in de workspace naar de AI-dienst gaat, en dat een Gebruiker kansen en projecten kan laten meegaan.
- Hij neemt passende maatregelen, zoals een instructie aan zijn Admins en Gebruikers, om te voorkomen dat het organisatieprofiel en de beschrijvingen van kansen en projecten die hij of zijn Gebruikers laten meegaan, bijzondere persoonsgegevens bevatten of meer persoonsgegevens dan nodig (AUP E.7). Het Platform toont daarvoor een waarschuwing en filtert niet op namen. Dit is een inspanningsverplichting en geen garantie voor het gedrag van individuele Gebruikers.
- Hij beoordeelt AI-uitvoer en elk voorstel vóór gebruik (Algemene Voorwaarden artikel 10) en gebruikt die niet voor de hoogrisicotoepassingen uit de AUP.
- Hij beoordeelt zelf of een DPIA nodig is en of instemming van de ondernemingsraad nodig is (art. 27 WOR).

4.11 **Wijziging.** Een andere aanbieder voor Deel A, een regio buiten de EU, een model buiten de Claude-modellen, een model met andere bewaring (artikel 4.8) of andere of extra gegevens uit de workspace dan artikel 4.3 noemt, volgt de procedure van artikel 5.2 van de Verwerkersovereenkomst.

4.12 **Uitzetten en nieuwe versie.**

- Zet de Admin de functie uit, dan stopt het sturen van Klantgegevens naar de AI-dienst direct, ook van het organisatieprofiel en de persoonlijke instructies. Bestaande gesprekken blijven bewaard volgens artikel 4.9.
- Een wijziging van deze module is wezenlijk als zij (a) een andere of extra Subverwerker voor Deel A betreft, (b) een regio buiten de zes regio's van artikel 4.5 of buiten de EU betreft, (c) andere of extra gegevens uit de workspace dan artikel 4.3 naar de AI-dienst stuurt, (d) de bewaring bij AWS of de modelaanbieder anders maakt dan artikel 4.8, (e) het model wijzigt (artikel 4.4), ook als het nieuwe model eerder is gebruikt of eerder in deze Bijlage werd genoemd, of (f) het doel wijzigt of het beschermingsniveau verlaagt. Verwerker kondigt een wezenlijke wijziging minstens 30 dagen vooraf aan, per e-mail aan de Admin(s) en met een melding in het Platform, met de nieuwe tekst, een samenvatting van wat verandert en de ingangsdatum (artikel 5.2 van de Verwerkersovereenkomst en artikel 16.1 van de Algemene Voorwaarden). Vanaf de ingangsdatum blijft de functie chat met AI voor de workspace uit tot een Admin de nieuwe versie heeft geaccepteerd. Artikel 16.3 van de Algemene Voorwaarden (stilzwijgende aanvaarding) geldt hiervoor niet. Een andere wijziging volgt artikel 16.1 van de Algemene Voorwaarden.

4.13 **Datalekken.** Artikel 8 van de Verwerkersovereenkomst geldt. AWS meldt een Security Incident zonder onredelijke vertraging nadat AWS ervan kennis heeft genomen, zonder termijn in uren (AWS DPA, artikel 9.1). Verwerker geeft die melding door volgens artikel 8.

4.14 **Rangorde.** Voor de verwerking in deze module (Deel A en Deel B) gaat deze Bijlage voor op de rest van de Verwerkersovereenkomst; voor het overige blijft de Verwerkersovereenkomst gelden (artikel 12).

4.15 **Organisatieprofiel.**

- **Wat.** Eén tekst per workspace van maximaal 2.000 tekens, geschreven door een Admin, met informatie over de organisatie die de AI kan helpen. Alleen voor de workspace van een bedrijf. Het profiel is leeg tot de Admin iets invult en wordt niet automatisch gevuld.
- **Gebruik.** Zolang deze module geldt, gaat het profiel mee als context bij elk gesprek van elke Gebruiker in de workspace. Dat geldt ook voor gesprekken met een eigen AI-koppeling (Deel B).
- **Wie leest en schrijft.** Alleen een Admin schrijft het. Elke Gebruiker met een lidmaatschap van de workspace leest het. Staff kan het lezen en schrijft het nooit, ook niet namens de Admin.

- **Bewaring.** Zolang de workspace bestaat, of tot de Admin het wist. Verwerker verwijdt het op de termijn van artikel 10.2.
- **Audit.** Elke wijziging legt het Platform vast met wie, wanneer, en de hash en de lengte van de oude en de nieuwe tekst. Nooit de tekst zelf. De Admin ziet dit in de audit-trail.

4.16 Persoonlijke instructies.

- **Wat.** Een tekst van maximaal 1.000 tekens per Gebruiker per workspace, met voorkeuren over toon, taal en opmaak van de antwoorden. Alleen voor de workspace van een bedrijf.
- **Gebruik.** De instructies gaan mee in de gesprekken van die Gebruiker in die workspace, naar de AI-dienst die voor het gesprek is gekozen.
- **Privé.** Alleen de Gebruiker zelf leest en schrijft ze. Andere Gebruikers, de Admin en Staff kunnen ze niet lezen. Voor Staff geldt artikel 3.3 op dezelfde manier als bij gesprekken, met de uitzonderingen van artikel 3.4 en 7 (gelogde procedure, op schriftelijke instructie van Verwerkingsverantwoordelijke).
- **Bewaring.** Tot de Gebruiker ze wist of het lidmaatschap van die Gebruiker in de workspace eindigt. Ze verdwijnen dan direct. Een later lidmaatschap start leeg.
- **Audit.** Alleen dat ze zijn opgeslagen of gewist, door wie en wanneer. Geen tekst, hash of lengte. De Admin ziet dit niet.

4.17 Kansen en projecten als context.

- **Per gesprek.** De Gebruiker kiest per gesprek of de AI niets krijgt (de standaard), alle kansen en projecten, of één kans of project. Het Platform slaat alleen die keuze op, niet de inhoud. Het stelt de context bij elke beurt opnieuw samen. Een verwijderd project valt dus weg.
- **Wat meegaat.** Per kans of project: de titel, de fase, of het een lighthouse is, de plaats op de kansenkaart, het aantal taken per status, de verwachte uitwerking en de beschrijving.
- **Wat niet.** Namen of gebruikers-ID's van wie een kans of project aanmaakte, beheert of kreeg toegewezen; titels of inhoud van taken; gearhiveerde kansen en projecten; bijlagen en documenten; chatberichten; gegevens van andere workspaces; projecten van klanten waar een partner aan werkt.
- **Rechten.** Alleen wat de Gebruiker zelf in het Platform mag zien en alleen met een lidmaatschap van die workspace. Staff zonder lidmaatschap kan niet chatten en dus geen context laden.
- **Vrije tekst.** Titel en beschrijving zijn vrije tekst en kunnen namen of andere persoonsgegevens bevatten. Die gaan dan mee. Het Platform waarschuwt daarvoor en filtert niet op namen. Alleen voor de workspace van een bedrijf, niet voor een partner-workspace.

4.18 Voorstellen voor een kans of taak.

- Het model kan in een antwoord een voorstel doen voor een nieuwe kans of een nieuwe taak, als tekst in een vast formaat. Het Platform toont dat als voorstel van de AI, met de tekst "Voorstel van de AI, nog niets aangemaakt".
- Het voorstel slaat niets op. Kiest de Gebruiker "Toevoegen", dan opent het gewone formulier voorgevuld. Pas als de Gebruiker daar zelf opslaat, ontstaat de kans of taak, met de rechten van die Gebruiker en met het gewone auditevent van die handeling. De Gebruiker kan alles aanpassen of weglaten.
- Het model kan niets aanmaken, wijzigen, archiveren of verwijderen, geen leden of instellingen wijzigen en niets anders uitvoeren (artikel 4.4). Het Platform neemt geen ID's of rechten uit een voorstel over.

- Een voorstel bindt Verwerkingsverantwoordelijke niet en is geen advies (Algemene Voorwaarden artikel 10).

Deel B

eigen AI-koppeling van de Klant

- 4.20 **Wat Deel B is.** De Admin kan een of meer eigen AI-accounts van de Klant koppelen onder Instellingen. De aanbieders staan in de keuzelijst in het Platform. Op het moment van deze versie zijn dat Azure OpenAI, OpenAI, Amazon Bedrock (in het eigen AWS-account van de Klant), Google Vertex AI (Anthropic-modellen) en Mistral AI. Een nieuwe aanbieder komt er alleen bij onder de voorwaarden van artikel 4.23. Deel B geldt vanaf het moment dat de Admin chat met AI inschakelt en deze module accepteert, en alleen voor gesprekken waarvoor de Gebruiker een eigen koppeling kiest.
- 4.21 **Rollen.** De Klant kiest de aanbieder, sluit zelf de overeenkomst en eventuele verwerkersovereenkomst met hem, gebruikt zijn eigen sleutel en is daarvoor verantwoordelijk. De aanbieder verwerkt de gegevens voor de Klant. Welke rol hij volgens zijn eigen voorwaarden voor zijn eigen doelen heeft, volgt uit de overeenkomst tussen de Klant en hem. Verwerker handelt bij het koppelen en bij elke aanroep uitsluitend op instructie van de Klant (de instelling van de Admin en de keuze van de Gebruiker per gesprek; artikel 2.2 van de Verwerkersovereenkomst) en is geen partij bij de overeenkomst tussen de Klant en de aanbieder. Verwerker schakelt de aanbieder niet in, geeft hem geen instructies en heeft geen overeenkomst met hem over deze verwerking. De aanbieder is daarom geen Subverwerker. De artikelen 5.2 en 5.3 gelden niet voor hem en hij staat niet in Bijlage 3. Verwerker blijft verwerker voor wat het Platform zelf doet: het samenstellen van de aanvraag, het versturen, het opslaan van het gesprek en de bewaring van de sleutel. Daarvoor gelden de Subverwerkers van Bijlage 3 (Supabase, Vercel).
- 4.22 **Wat het Platform verstuurt en ontvangt.** Het Platform stuurt naar de gekozen aanbieder hetzelfde als in Deel A: het gesprek (artikel 4.3) en, als artikel 4.15 tot en met 4.17 gelden, het organisatieprofiel, de persoonlijke instructies van de Gebruiker en de gekozen kansen en projecten. Het Platform ontvangt de antwoordtekst en het aantal gebruikte tokens. Direct na het koppelen en bij "Opnieuw testen" stuurt het Platform een vaste, synthetische testtekst zonder gegevens uit de workspace. Het gesprek slaat het Platform op zoals in artikel 4.9. Verwerker test de koppelingen met een eigen account bij de aanbieder, uitsluitend met synthetische gegevens zonder persoonsgegevens en zonder Klantgegevens. Voor die tests is de aanbieder geen Subverwerker.
- 4.23 **Alleen naar een Europees eindpunt.** Het Platform stuurt alleen naar een Europees eindpunt van de aanbieder en nooit naar een eindpunt dat het niet als Europees herkent, ook niet als de Admin dat bevestigt. Bij het opslaan van de koppeling én bij elke aanroep controleert het Platform dat: de regio in de lijst met Europese regio's van de aanbieder staat en het implementatietype niet "global" is; het eindpunt exact een toegestane hostnaam van die aanbieder is (alleen https, geen IP-adres, geen poort, geen gebruikersinfo, geen pad of query); het model of de implementatie aan het patroon van de aanbieder voldoet; er geen doorverwijzing wordt gevolgd. Anders weigert het Platform de aanroep. Deze controle is een technische en organisatorische maatregel ten behoeve van de Klant. Ze geeft Verwerker geen zeggenschap over het doel of de middelen van de verwerking door de aanbieder.
- 4.24 **Wat het Platform niet kan controleren.** De Admin bevestigt bij het koppelen dat hij een Europees eindpunt of een Europese regio koos. Het Platform legt de datum van die bevestiging vast. Het Platform kan niet zien, en de Admin beoordeelt zelf: het implementatietype van een Azure-implementatie, dat een OpenAI-project Europese dataresidentie heeft, het plan en de trainingsinstelling bij Mistral, de bestemmingsregio's van een eigen Europees inferentieprofiel bij Amazon Bedrock, en wat de aanbieder bewaart of logt. Verwerker belooft niet dat de aanbieder uitsluitend in de EU verwerkt of bewaart. Wat de aanbieder doet, volgt uit zijn overeenkomst met de Klant (artikel 4.28).

- 4.25 **Sleutels.** De sleutel van de Klant staat in Supabase Vault (Frankfurt). Het Platform bewaart verder alleen de laatste vier tekens als hint. Een sleutel gaat nooit naar de browser, naar logs of naar een audit-gebeurtenis. De Admin kan een sleutel vernieuwen of intrekken; een ingetrokken koppeling wordt niet meer gebruikt.
- 4.26 **Keuze per gesprek, geen terugval.** De Gebruiker kiest per gesprek welke koppeling het gebruikt: de AI van Verwerker (Deel A) of een eigen koppeling. Het Platform wisselt nooit stilzwijgend van koppeling. Is een gekozen koppeling niet bruikbaar, dan weigert het Platform het gesprek. Kiest een Gebruiker voor een gesprek de AI van Verwerker, dan geldt Deel A voor dat gesprek en is Amazon Web Services EMEA SARL de Subverwerker, ook als de Admin ook eigen koppelingen heeft toegevoegd. De acceptatie van deze module dekt dat.
- 4.27 **Audit en meting.** Het Platform legt het koppelen, vernieuwen en intrekken van een koppeling en wijzigingen aan de keuzelijst vast als `ai_provider_config_changed`, zonder sleutel, hint of host. Het telt per maand, koppeling en model het aantal aanroepen en tokens, zonder inhoud en zonder Gebruiker.
- 4.28 **Bewaring en training bij de aanbieder.** Wat de aanbieder bewaart, logt, beoordeelt of voor training gebruikt, volgt de overeenkomst tussen de Klant en de aanbieder. De artikelen 4.5 tot en met 4.8 en 4.13 gelden niet voor de aanbieder. Verwerker gebruikt invoer en uitvoer zelf niet om modellen te trainen (artikel 2.5). Met acceptatie van deze module bevestigt Verwerkingsverantwoordelijke dat hij dit verschil kent.
- 4.29 **Verplichtingen van de Verwerkingsverantwoordelijke (Deel B).** Hij beoordeelt de aanbieder, zijn verwerkersovereenkomst en de instellingen daar (waaronder training uit, bewaring en logging) vóór hij koppelt. Artikel 4.10 geldt ook voor Deel B.

Historie

Wijzigingshistorie

1.7 · huidig	30 sep 2026	Bijlage 4 (Module AI-verwerking) is versie 1.4: het AI-model is een model van Anthropic via AWS Bedrock; de actuele modelnaam staat op de pagina Datalocatie, een wijziging kondigen wij 30 dagen vooraf aan en is een wezenlijke wijziging met bezwaarrecht (4.4, 4.12). Partnertoegang wordt verlengd, niet opnieuw gekozen (3.5). Chat met AI blijft uit tot een admin versie 1.4 accepteert.
Versie 1.6	30 sep 2026	Nieuw: toegang van een partner tot één project na jouw keuze, voor ten hoogste 6 maanden (artikel 3.5). De persoonsgegevens heten nu Klantgegevens. Aanvullingen in bijlage 1 tot en met 3 (onder meer Supabase, Brevo en Exact). Bijlage 4 (Module AI-verwerking) is versie 1.3, inhoudelijk gelijk. Chat met AI blijft uit tot een admin versie 1.3 accepteert.
Versie 1.5	30 sep 2026	Bijlage 4 (Module AI-verwerking) is versie 1.2: je geeft met de acceptatie de instructie voor de AI-verwerking (4.1), een duidelijke omschrijving van een wezenlijke wijziging met 30 dagen aankondiging (4.12), een regeling voor Claude Sonnet (4.4), een eigen AI-koppeling blijft jouw verwerker en testen van Norwin gebeurt alleen met synthetische gegevens (4.21 tot en met 4.24). Ook artikel 5.5, 10.3 en bijlage 1 en 3. Chat met AI blijft uit tot een admin versie 1.2 accepteert.
Versie 1.4	30 sep 2026	Bijlage 4 (Module AI-verwerking) is versie 1.1: organisatieprofiel, persoonlijke instructies, kansen en projecten als context, voorstellen voor kansen en taken, en eigen AI-koppelingen van de klant (geen subverwerker). Aanpassingen ook in artikel 3.2 tot en met 3.4, 5.5, 5.6, 7, 10.2 en bijlage 1 tot en met 3. Chat met AI

blijft uit tot een admin de nieuwe versie van de module accepteert. Lees de wijzigingen via de link bij deze melding.

Versie 1.3	30 sep 2026	Nieuwe Bijlage 4 (Module AI-verwerking, apart te accepteren bij het inschakelen van chat met AI) en een nieuwe subverwerker: Amazon Web Services EMEA SARL (Amazon Bedrock), alleen voor workspaces waar chat met AI aan staat, in regio's binnen de EU. Gesprekken zijn persoonlijk en blijven bewaard zolang de workspace bestaat. Aanpassingen in artikel 3.3, 5.5, 7, 9.1, 10.2 en bijlage 1 tot en met 4. Bezwaar: mail info@norwin.ai (artikel 5.2).
Versie 1.2	30 sep 2026	Extra, optionele inlogroute: inloggen met een Google-account (Bijlage 1, 2 en 3). Wie toegang heeft tot jullie Workspace verandert niet en er gaan geen Workspace-gegevens naar Google; lidmaatschap blijft onder beheer van de Admin en ontstaat pas na bevestiging van de mailbox. Lees de wijzigingen via de link bij deze melding. Past dit niet bij jullie, mail info@norwin.ai ; je kunt de overeenkomst dan kosteloos opzeggen.
Versie 1.1	30 sep 2026	Extra, optionele inlogroute: inloggen met een Microsoft-werk- of schoolaccount (Bijlage 1, 2 en 3). Wie toegang heeft tot jullie Workspace verandert niet en er gaan geen Workspace-gegevens naar de provider; lidmaatschap blijft onder beheer van de Admin en ontstaat pas na bevestiging van de mailbox. De Admin kan de route niet uitzetten. Geen nieuwe acceptatie nodig (art. 16.4).
Versie 1.0	30 sep 2026	Eerste definitieve versie: logboek databasetoegang, incidentprocedure, back-ups, tokens uit GitHub, subverwerkers.

Vragen over dit document? Mail info@norwin.ai.