

Verwerkersovereenkomst

Deze verwerkersovereenkomst legt vast hoe DataFlowr persoonsgegevens verwerkt in opdracht van zijn klanten, zoals artikel 28 lid 3 AVG voorschrijft. Zij hoort bij elke overeenkomst op grond waarvan DataFlowr persoonsgegevens verwerkt, waaronder het gebruik van Claire. Dit document is ook beschikbaar in het Engels; bij verschil in uitleg is de Nederlandse tekst leidend.

VERSIE 1.0 · AUGUSTUS 2026

Partijen

1. DataFlowr B.V., gevestigd aan de Van Marsbergenstraat 71, 2134 LV Hoofddorp, ingeschreven bij de Kamer van Koophandel onder nummer 99021145, hierna “DataFlowr”, “wij” of “ons”;
2. de klant die een Overeenkomst met DataFlowr heeft gesloten, hierna “de Klant” of “je”.

Overwegingen

- A. Wij leveren Claire, de AI-laag boven op Exact Online, en consultancydiensten binnen het Exact Online ecosysteem. Daarbij verwerken wij persoonsgegevens in opdracht van de Klant, waaronder de gegevens die Claire per vraag uit de gekoppelde Exact Online-administratie ophaalt.
- B. Voor die verwerkingen bepaalt de Klant het doel en de middelen. De Klant is verwerkingsverantwoordelijke in de zin van artikel 4 sub 7 AVG en wij zijn verwerker in de zin van artikel 4 sub 8 AVG.
- C. In deze Verwerkersovereenkomst leggen we de afspraken vast die artikel 28 lid 3 AVG voorschrijft. De drie bijlagen horen bij deze Verwerkersovereenkomst: Bijlage 1 beschrijft de verwerking, Bijlage 2 de beveiligingsmaatregelen en Bijlage 3 de subverwerkers.

Partijen komen het volgende overeen.

Artikel 1 · Definities

- 1.1 Begrippen uit de AVG, zoals verwerking, persoonsgegevens, verwerkingsverantwoordelijke, verwerker, betrokkene en inbreuk in verband met persoonsgegevens, hebben in deze Verwerkersovereenkomst de betekenis die de AVG daaraan geeft.
- 1.2 AVG: Verordening (EU) 2016/679 (algemene verordening gegevensbescherming) en de Uitvoeringswet AVG.
- 1.3 Overeenkomst: elke overeenkomst tussen DataFlowr en de Klant op grond waarvan wij de Dienst leveren, waaronder de algemene voorwaarden en een offerte of opdrachtbevestiging.
- 1.4 Dienst: Claire, het abonnement op de AI-laag boven op de eigen Exact Online-administratie van de Klant, en de consultancydiensten waarbij wij toegang hebben tot persoonsgegevens.
- 1.5 Persoonsgegevens: de persoonsgegevens die wij in opdracht van de Klant verwerken bij het leveren van de Dienst, zoals omschreven in Bijlage 1.

- 1.6 Betrokkene: degene op wie een Persoonsgegevens betrekking heeft.
- 1.7 Datalek: een inbreuk in verband met persoonsgegevens zoals bedoeld in artikel 4 sub 12 AVG.
- 1.8 Subverwerker: een andere verwerker die wij inschakelen om ten behoeve van de Klant specifieke verwerkingsactiviteiten te verrichten.
- 1.9 Verwerkersovereenkomst: deze verwerkersovereenkomst, inclusief de drie bijlagen.

Artikel 2 · Rolverdeling en reikwijdte

- 2.1 Deze Verwerkersovereenkomst geldt voor iedere verwerking van Persoonsgegevens die wij uitvoeren bij het leveren van de Dienst. Zij maakt deel uit van de Overeenkomst en hoeft niet apart te worden ondertekend. Wil je een ondertekend exemplaar, gebruik dan de ondertekenpagina achter artikel 14.
- 2.2 De Klant is verwerkingsverantwoordelijke en bepaalt het doel en de middelen van de verwerking. Wij zijn verwerker en verwerken uitsluitend in opdracht van de Klant.
- 2.3 Is de Klant zelf verwerker voor een derde, bijvoorbeeld als accountants- of administratiekantoor dat de administratie van een cliënt voert, dan treden wij op als subverwerker. Deze Verwerkersovereenkomst geldt dan onverkort. De Klant staat er in dat geval voor in dat zijn afspraken met de verwerkingsverantwoordelijke het inschakelen van DataFlowr toestaan en dat de instructies die hij ons geeft binnen die afspraken passen.
- 2.4 De Klant staat ervoor in dat de verwerking van de Persoonsgegevens rechtmatig is: dat er een grondslag is, dat Betrokkenen waar nodig zijn geïnformeerd en dat de inhoud van de gegevens en de manier waarop zij zijn verkregen niet onrechtmatig zijn.
- 2.5 Wij laten de Klant meteen weten wanneer een instructie naar ons oordeel in strijd is met de AVG of met andere privacywetgeving.

Artikel 3 · Instructies en verwerking

- 3.1 Wij verwerken de Persoonsgegevens uitsluitend op basis van gedocumenteerde instructies van de Klant, ook waar het doorgifte aan een land buiten de EER betreft, tenzij een Unierechtelijke of Nederlandse wettelijke bepaling ons tot verwerking verplicht. In dat laatste geval melden wij dat vooraf, tenzij die wetgeving dat verbiedt. De Overeenkomst, deze Verwerkersovereenkomst en het gebruik en de instellingen van de Dienst, zoals welke administraties zijn gekoppeld, welke modules aanstaan en welke vragen worden gesteld, gelden samen als die instructies.
- 3.2 Wij verwerken de Persoonsgegevens niet voor eigen doeleinden. Wij verkopen ze niet, gebruiken ze niet voor advertenties en trainen er geen AI-modellen op. Onze modelaanbieders verwerken prompts alleen om te antwoorden; trainen op klantgegevens is contractueel uitgesloten.
- 3.3 Wij verwerken niet langer of uitgebreider dan voor de Dienst nodig is. Claire haalt gegevens per vraag op uit de gekoppelde administratie; er ontstaat geen kopie van de administratie buiten Exact Online. Een wijziging in de administratie voeren wij pas uit nadat de gebruiker die uitdrukkelijk heeft goedgekeurd.
- 3.4 Alleen medewerkers voor wie dat voor hun werk noodzakelijk is hebben toegang tot Persoonsgegevens, en niet verder dan voor dat werk nodig is.
- 3.5 Krijgen wij van een bevoegde instantie een verzoek om Persoonsgegevens te verstrekken, dan beoordelen wij eerst of het verzoek bindend is. Wij informeren de Klant vóór verstrekking, tenzij de wet dat verbiedt, en zo tijdig dat de Klant rechtsmiddelen kan instellen.

Artikel 4 · Geheimhouding

- 4.1 Wij houden de Persoonsgegevens vertrouwelijk. Iedereen die onder ons gezag Persoonsgegevens verwerkt, heeft zich schriftelijk tot geheimhouding verplicht of is gebonden aan een wettelijke geheimhoudingsplicht.
- 4.2 De geheimhouding geldt niet voor zover de Klant toestemming heeft gegeven voor verstrekking, verstrekking nodig is voor de Dienst of een wettelijke plicht tot verstrekking bestaat.
- 4.3 Dit artikel blijft gelden nadat de Verwerkersovereenkomst is geëindigd.

Artikel 5 · Beveiliging

- 5.1 Wij treffen passende technische en organisatorische maatregelen zoals bedoeld in artikel 32 AVG, rekening houdend met de stand van de techniek, de uitvoeringskosten en de aard, omvang, context en doeleinden van de verwerking en de risico's voor Betrokkenen. De maatregelen staan in Bijlage 2.
- 5.2 Financiële gegevens zijn persoonsgegevens van gevoelige aard. Het beveiligingsniveau van de Dienst is daarop afgestemd.
- 5.3 Wij evalueren de maatregelen periodiek en scherpen ze aan wanneer de risico's of de stand van de techniek daarom vragen. Wij mogen Bijlage 2 aanpassen, zolang het geheel aan maatregelen geen lager beschermingsniveau biedt.
- 5.4 Op verzoek geven wij de Klant de informatie die nodig is om te beoordelen of de maatregelen passend zijn.

Artikel 6 · Subverwerkers

- 6.1 De Klant geeft ons algemene toestemming om Subverwerkers in te schakelen bij het leveren van de Dienst. De actuele lijst staat in Bijlage 3.
- 6.2 Wij leggen iedere Subverwerker schriftelijk verplichtingen op het gebied van gegevensbescherming op die minimaal gelijkwaardig zijn aan onze verplichtingen onder deze Verwerkersovereenkomst, waaronder geheimhouding, beveiliging en de regels voor doorgifte.
- 6.3 Een nieuwe of vervangende Subverwerker kondigen wij ten minste 30 dagen van tevoren per e-mail aan bij de contactpersoon van het account. De actuele lijst publiceren wij daarnaast in dit document op onze website.
- 6.4 De Klant kan binnen 14 dagen na de aankondiging schriftelijk bezwaar maken op redelijke, onderbouwde gronden die met gegevensbescherming te maken hebben. We zoeken dan samen naar een redelijke oplossing. Komt die er niet, dan mag de Klant het geraakte deel van de Dienst opzeggen tegen de datum waarop de wijziging ingaat.
- 6.5 Wij blijven tegenover de Klant volledig verantwoordelijk voor het nakomen van de verplichtingen door onze Subverwerkers, zoals artikel 28 lid 4 AVG bepaalt.
- 6.6 Exact Online is geen Subverwerker van ons: de Klant koppelt zijn eigen administratie via zijn eigen overeenkomst met Exact en zijn eigen Exact Online-account. Hetzelfde geldt voor een AI-client die de Klant zelf kiest, zoals Claude, ChatGPT of Microsoft Copilot, en voor een eigen AI-aanbieder of eigen API-sleutel die de Klant zelf instelt: die vallen onder de afspraken van de Klant met die aanbieder.

Artikel 7 · Doorgifte buiten de EER

- 7.1 Een deel van onze Subverwerkers verwerkt Persoonsgegevens ook buiten de Europese Economische Ruimte, met name in de Verenigde Staten. Bijlage 3 vermeldt dat per Subverwerker.

- 7.2 Doorgifte naar een land buiten de EER vindt alleen plaats in overeenstemming met hoofdstuk V van de AVG (artikelen 44 t/m 49): op basis van een adequaatheidsbesluit van de Europese Commissie, waaronder het EU-VS Data Privacy Framework voor ontvangers die daaronder gecertificeerd zijn, of met passende waarborgen zoals de standaardcontractbepalingen van de Europese Commissie (Uitvoeringsbesluit (EU) 2021/914), waar nodig met aanvullende maatregelen.
- 7.3 Wij geven Persoonsgegevens niet op eigen initiatief door aan andere landen of ontvangers dan in Bijlage 3 vermeld.

Artikel 8 · Bijstand bij rechten van betrokkenen

- 8.1 Krijgen wij een verzoek of klacht van een Betrokkene over Persoonsgegevens, bijvoorbeeld om inzage of verwijdering, dan sturen wij dat binnen drie werkdagen door aan de Klant, zonder er zelf inhoudelijk op te reageren.
- 8.2 Rekening houdend met de aard van de verwerking helpen wij de Klant met passende technische en organisatorische maatregelen om te voldoen aan verzoeken van Betrokkenen op grond van hoofdstuk III AVG, waaronder inzage, rectificatie, wissing, beperking, bezwaar en overdraagbaarheid. Veel kan de Klant zelf: gesprekken zijn in de applicatie in te zien en te verwijderen en de koppeling is direct in te trekken. Wat de Klant niet zelf kan, doen wij op verzoek via privacy@dataflowr.nl.
- 8.3 Deze bijstand is kosteloos. Alleen wanneer verzoeken structureel of buitensporig zijn, mogen wij er redelijke kosten voor in rekening brengen; dat melden we vooraf.

Artikel 9 · Datalekken

- 9.1 Ontdekken wij een Datalek dat de Persoonsgegevens raakt, dan melden wij dat zonder onredelijke vertraging aan de Klant, en uiterlijk binnen 48 uur nadat wij het hebben vastgesteld. We melden aan de contactpersoon van het account, op het e-mailadres dat daarvoor bij ons bekend is.
- 9.2 De melding bevat, voor zover dan bekend: de aard van het Datalek, de categorieën Betrokkenen en registers die het raakt en bij benadering de aantallen, de waarschijnlijke gevolgen, de maatregelen die we hebben genomen of voorstellen, en ons contactpunt privacy@dataflowr.nl. Informatie die later beschikbaar komt, leveren we in stappen na.
- 9.3 De beoordeling en de melding aan de Autoriteit Persoonsgegevens en aan Betrokkenen zijn aan de Klant als verwerkingsverantwoordelijke. Wij helpen de Klant bij het nakomen van die meldplicht (artikelen 33 en 34 AVG) en melden zelf niet, tenzij de wet ons daartoe verplicht.
- 9.4 Wij documenteren ieder Datalek dat de Persoonsgegevens raakt: de feiten, de gevolgen en de genomen maatregelen.

Artikel 10 · Bijstand bij DPIA en voorafgaande raadpleging

- 10.1 Rekening houdend met de aard van de verwerking en de informatie waarover wij beschikken, helpen wij de Klant redelijkerwijs bij een gegevensbeschermingseffectbeoordeling (artikel 35 AVG) en bij een voorafgaande raadpleging van de Autoriteit Persoonsgegevens (artikel 36 AVG).

Artikel 11 · Informatie en audit

- 11.1 Op verzoek stellen wij de Klant alle informatie ter beschikking die nodig is om aan te tonen dat wij artikel 28 AVG en deze Verwerkersovereenkomst nakomen: documentatie over onze maatregelen, de bijlagen bij dit

document en, wanneer beschikbaar, rapportages van onafhankelijke derden.

- 11.2 De Klant mag daarnaast een audit laten uitvoeren, door zichzelf of door een onafhankelijke deskundige die tot geheimhouding is verplicht. Een audit vindt hoogstens eenmaal per twaalf maanden plaats, na een schriftelijke aankondiging van ten minste 30 dagen, tijdens kantooruren en zonder de bedrijfsvoering onnodig te verstoren. De audit geeft geen toegang tot gegevens van andere klanten. De beperking tot eenmaal per twaalf maanden geldt niet wanneer daar een concrete aanleiding voor is, zoals een Datalek dat de Persoonsgegevens raakt of een onderbouwd vermoeden dat wij deze Verwerkersovereenkomst niet nakomen.
- 11.3 De kosten van een audit draagt de Klant. Blijkt uit de audit dat wij wezenlijk tekortschieten, dan dragen wij onze eigen redelijke kosten van medewerking.
- 11.4 De bevindingen behandelen beide partijen vertrouwelijk. Gerechtaardigde verbeterpunten voeren wij binnen een redelijke termijn door.
- 11.5 Beide partijen werken desgevraagd samen met de Autoriteit Persoonsgegevens bij het vervullen van haar taken.

Artikel 12 · Aansprakelijkheid

- 12.1 De regeling van aansprakelijkheid in de Overeenkomst geldt ook voor deze Verwerkersovereenkomst.
- 12.2 Onverminderd artikel 12.1 draagt ieder van ons de schade en de boetes van de toezichthouder die voortvloeien uit het eigen niet-nakomen van de AVG of van deze Verwerkersovereenkomst.

Artikel 13 · Duur, einde en verwijdering

- 13.1 Deze Verwerkersovereenkomst geldt zolang de Overeenkomst loopt, en daarna zolang wij nog Persoonsgegevens verwerken in het kader van de Dienst.
- 13.2 Na het einde van de Overeenkomst verwijderen wij alle Persoonsgegevens, inclusief kopieën, binnen 90 dagen. Vraagt de Klant vóór dat moment om teruggave, dan leveren wij de Persoonsgegevens eerst in een gangbaar bestandsformaat aan. Verwijdering werkt door in back-ups volgens het rotatieschema van het hostingplatform.
- 13.3 De verwijderplicht geldt niet voor zover een Unierechtelijke of Nederlandse wettelijke bepaling ons tot bewaren verplicht. Die gegevens bewaren we niet langer dan die plicht vereist.
- 13.4 Trekt de Klant de koppeling met Exact Online in, dan vervallen de toegangstokens meteen en verwijderen wij ze. De gegevens in de Exact Online-administratie zelf blijven onaangetast bij Exact staan; daarover gaat de eigen overeenkomst van de Klant met Exact.
- 13.5 Bepalingen die naar hun aard doorlopen, zoals geheimhouding en aansprakelijkheid, blijven ook na het einde gelden.

Artikel 14 · Slotbepalingen

- 14.1 Bij strijd tussen deze Verwerkersovereenkomst en de Overeenkomst gaat deze Verwerkersovereenkomst voor, voor zover het de verwerking van Persoonsgegevens betreft.
- 14.2 Wijzigd de Dienst, de lijst van Subverwerkers of de wet, dan passen wij dit document aan. De nieuwe versie publiceren wij op dataflowr.nl met een nieuw versienummer en een nieuwe datum. Een wijziging die de

rechten van de Klant wezenlijk raakt, kondigen wij ten minste 30 dagen van tevoren aan; kan de Klant zich er niet in vinden, dan mag hij de Overeenkomst opzeggen tegen de datum waarop de wijziging ingaat.

- 14.3** Is een bepaling van deze Verwerkersovereenkomst ongeldig, dan blijven de overige bepalingen gelden. Partijen vervangen de ongeldige bepaling door een geldige die de strekking zo dicht mogelijk benadert.
- 14.4** Op deze Verwerkersovereenkomst is Nederlands recht van toepassing. Geschillen leggen we voor aan de bevoegde rechter in Noord-Holland, tenzij de wet een andere rechter aanwijst.
- 14.5** Deze Verwerkersovereenkomst bestaat in een Nederlandse en een Engelse versie. Bij verschil in uitleg is de Nederlandse tekst leidend.
- 14.6** Mededelingen onder deze Verwerkersovereenkomst doe je aan privacy@dataflowr.nl. Wij gebruiken de contactgegevens van het account van de Klant.

Ondertekening

Deze Verwerkersovereenkomst geldt als onderdeel van de Overeenkomst, ook zonder handtekening. Wil je een ondertekend exemplaar, vul dan hieronder beide kolommen in en stuur het document naar privacy@dataflowr.nl. Wij sturen een getekend exemplaar terug.

DataFlowr B.V.

NAAM

FUNCTIE

DATUM

HANDTEKENING

De Klant

BEDRIJFSNAAM

NAAM

FUNCTIE

DATUM

HANDTEKENING

Specificatie van de verwerking

Onderwerp en aard van de verwerking

Wij leveren Claire, de AI-laag boven op de eigen Exact Online-administratie van de Klant. Gebruikers stellen vragen in gewone taal; Claire haalt per vraag de benodigde gegevens uit de gekoppelde administratie op, stelt met een taalmodel een antwoord op en voert een wijziging pas uit na uitdrukkelijk akkoord van de gebruiker. Daarnaast draaien er op verzoek van de Klant geautomatiseerde controles en planningen, zoals de maandafsluitingscontroles en de cashflowprognose, en versturen wij e-mailnotificaties over de uitkomsten. Bij consultancy-opdrachten verwerken wij daarnaast de persoonsgegevens waartoe de Klant ons voor de opdracht toegang geeft.

Doel van de verwerking

Uitsluitend het leveren van de Dienst zoals in de Overeenkomst omschreven: vragen beantwoorden, goedgekeurde wijzigingen doorvoeren, controles en planningen draaien, de Klant ondersteunen en de beveiliging van het platform bewaken.

Duur

Zolang de Overeenkomst loopt, en daarna tot de verwijdering van artikel 13 is afgerond.

Categorieën van betrokkenen

- Gebruikers en medewerkers van de Klant die met de Dienst werken.
- Contactpersonen, klanten en leveranciers van de Klant, waaronder debiteuren en crediteuren, en hun medewerkers, voor zover hun gegevens in de gekoppelde administratie staan.
- Overige personen van wie gegevens voorkomen in de gekoppelde administratie, in gestelde vragen of in geüploade bestanden.

Categorieën van persoonsgegevens

CATEGORIE	GEGEVENS
Accountgegevens	Naam, e-mailadres, profielfoto en de identiteit van de inlogmethode.
Koppelingsgegevens	OAuth-toegangstokens voor Exact Online en welke administraties zijn gekoppeld.
Gespreksgegevens	Vragen, antwoorden, de per vraag opgehaalde gegevens en bestanden die gebruikers uploaden.
Administratiegegevens	Naam-, adres- en contactgegevens en financiële gegevens uit de gekoppelde administratie, zoals facturen, openstaande posten, transacties en bankgegevens, voor zover een vraag of controle ze ophaalt.
Logs	Welke actie wanneer en onder welk account is uitgevoerd, IP-adres, tijdstip en de gebruikte client.

De Dienst is niet bedoeld voor bijzondere categorieën van persoonsgegevens (artikel 9 AVG) of strafrechtelijke gegevens. Staan die toch in de administratie, in vragen of in bestanden, dan gelden de maatregelen van Bijlage 2 onverkort. Financiële gegevens zijn persoonsgegevens van gevoelige aard; de beveiliging is daarop afgestemd.

Facturatiegegevens van de Klant zelf, zoals bedrijfsnaam, btw-nummer en factuurhistorie, verwerken wij voor onze eigen facturatie en boekhouding. Daarvoor zijn wij verwerkingsverantwoordelijke; die verwerking valt onder onze privacyverklaring, niet onder deze Verwerkersovereenkomst.

Bewaartermijnen

GEGEVENS	TERMIJN
Account en gesprekken	Zolang het abonnement loopt. Het transcript van een gesprek (vragen, antwoorden en opgehaalde gegevens) wordt daarnaast standaard 30 dagen na het laatste gebruik automatisch verwijderd; geüploade bestanden verdwijnen wanneer het gesprek wordt verwijderd. Na het einde van de Overeenkomst verwijderen wij account, gesprekken en bestanden binnen 90 dagen.
Koppelingsgegevens	Tot de Klant de koppeling intrekt of de Overeenkomst eindigt; daarna vervallen de tokens en verwijderen wij ze.
Logs	Twaalf maanden, zodat een incident achteraf te onderzoeken is. Na het einde van de Overeenkomst geldt bovendien de termijn van artikel 13.

Rechten en verplichtingen van de Klant

De Klant blijft verwerkingsverantwoordelijke: hij zorgt voor een grondslag, informeert Betrokkenen waar nodig, geeft instructies die met de AVG stroken en beheert zelf de gebruikers en toegangsrechten in zijn Exact Online-administratie. De koppeling loopt via het eigen Exact Online-account van iedere gebruiker: Claire kan precies wat die gebruiker in Exact Online mag, niets meer.

Technische en organisatorische maatregelen

Deze maatregelen beschrijven wat de Dienst vandaag doet. Wij evalueren ze periodiek en mogen ze aanpassen zolang het beschermingsniveau er niet op achteruitgaat (artikel 5).

Versleuteling en sleutelbeheer

- Al het verkeer met de applicatie en met Exact Online loopt over TLS (1.2 of hoger).
- De koppeling met Exact Online verloopt via OAuth; wij ontvangen en bewaren geen Exact Online-wachtwoorden.
- ERP-toegangstokens, client secrets en API-sleutels worden met AES-256-GCM versleuteld opgeslagen, met ondersteuning voor sleutelrotatie.
- Langlevende toegangstokens en uitnodigingstokens worden als SHA-256-hash bewaard; het token zelf is eenmalig zichtbaar.

Toegang en autorisatie

- Inloggen loopt via onze identiteitsleverancier op een Europese omgeving, met ondersteuning voor meerfactorauthenticatie en passkeys. Sessies verlopen na 24 uur.
- Toegang is gescheiden per organisatie. Een koppeling is alleen bereikbaar voor leden van de organisatie, en ieder lid autoriseert met zijn eigen Exact Online-account: Claire kan per gebruiker precies wat die gebruiker in Exact Online mag.
- Beheerhandelingen, zoals het verwijderen van een koppeling, kunnen alleen beheerders uitvoeren. Per koppeling zijn modules en tools aan of uit te zetten; die instellingen worden bij elke uitvoering afgedwongen.
- Schrijfacties naar Exact Online vereisen altijd een expliciet akkoord van de gebruiker en worden zo vastgelegd dat een actie nooit twee keer wordt uitgevoerd.
- Toegang tot productiesystemen is beperkt tot de medewerkers die hem nodig hebben. Het interne beheerdashboard toont alleen geaggregeerde cijfers, geen administratiegegevens.

Logging en controle

- Elke tooluitvoering wordt gelogd met gebruiker, tijdstip en gebruikte client. Het auditlog is voor de Klant in de applicatie in te zien.
- Voor lijst- en schrijftools bevat het auditlog samenvattingen in plaats van volledige resultaten.
- Geheimen worden uit logregels geredigeerd; serverlogs bevatten geen toegangstokens.

Dataminimalisatie richting AI-modellen

- Claire haalt gegevens per vraag op; er ontstaat geen kopie van de administratie buiten Exact Online.
- Richting de AI-gateway wordt de gebruiker pseudoniem doorgegeven: een interne code, geen naam of e-mailadres.
- Op het niveau van de AI-gateway is redactie geconfigureerd: e-mailadressen, telefoonnummers en creditcardnummers worden geredigeerd voordat een prompt de modelaanbieder bereikt. In de maandafsluitingscontroles maskeert de applicatie daarnaast IBAN's en e-mailadressen.
- Wij trainen geen AI-modellen op klantgegevens. Voor onze modelaanbidders is trainen op klantgegevens contractueel uitgesloten.

Applicatie- en platformbeveiliging

- Beveiligingsheaders (waaronder een strikte Content Security Policy en HSTS), CSRF-bescherming en rate limiting op de API.
- Geautomatiseerde beveiligingscontroles in de ontwikkelpijplijn: afhankelijkheidscontrole, statische analyse en baseline-scans.
- Een gecoördineerde meldprocedure voor kwetsbaarheden, gepubliceerd via security.txt.
- De applicatie draait op een beheerd cloudplatform; back-ups van database en objectopslag lopen via de voorzieningen van dat platform.

Organisatie

- Medewerkers zijn tot geheimhouding verplicht en krijgen alleen de toegang die hun werk vereist.
- Wij beoordelen periodiek of de maatregelen nog passen bij de risico's en de stand van de techniek.

Subverwerkers

Wij schakelen de volgende Subverwerkers in. Wijzigingen kondigen wij aan volgens artikel 6. Met iedere Subverwerker hebben wij een verwerkersovereenkomst of gelijkwaardige contractuele afspraken.

SUBVERWERKER	DIENST	LOCATIE	DOORGIFTEMECHANISME
Auth0 (Okta, Inc.)	Inloggen en accountbeheer	EU-omgeving; moederbedrijf VS	EU-VS Data Privacy Framework
Replit, Inc.	Hosting van applicatie en database	VS; infrastructuur op Google Cloud	Standaardcontractbepalingen
Google LLC (Google Cloud)	Cloudinfrastructuur en opslag van werkbestanden	EU en VS	EU-VS Data Privacy Framework
OpenRouter, Inc.	AI-gateway die vragen naar het gekozen taalmodel routeert	VS	Standaardcontractbepalingen
De geselecteerde modelaanbieder (zoals Google, OpenAI of Anthropic)	Het opstellen van antwoorden, via OpenRouter	Afhankelijk van het gekozen model, EER of VS	Standaardcontractbepalingen of een eigen DPF-certificering, vastgelegd tussen OpenRouter en de aanbieder
Resend, Inc.	E-mailnotificaties	VS	EU-VS Data Privacy Framework

Geen Subverwerkers

- Exact Online: de Klant koppelt zijn eigen administratie via zijn eigen overeenkomst met Exact en zijn eigen Exact Online-account. Exact verwerkt niet in onze opdracht.
- AI-clients die de Klant zelf kiest, zoals Claude, ChatGPT of Microsoft Copilot: vragen en antwoorden lopen dan ook door die client. Dat valt onder de overeenkomst van de Klant met die aanbieder.
- Een eigen AI-aanbieder of eigen API-sleutel die de Klant zelf instelt: die aanbieder is dan een verwerker van de Klant. Onze platformsleutel wordt daarbij nooit meegestuurd.
- Stripe verwerkt de betalingen van het abonnement voor onze eigen facturatie. Daarvoor zijn wij verwerkingsverantwoordelijke; die verwerking valt onder onze privacyverklaring.