Je Autorespond koppelen aan je AI-assistent (FluentCRM MCP): veilig en volgens de AVG

Integraties · https://autorespond.nl/docs/autorespond-koppelen-aan-je-ai-assistent-fluentcrm-mcp/

Met de MCP-koppeling (Model Context Protocol) laat je jouw AI-assistent, bijvoorbeeld Claude of ChatGPT, rechtstreeks meekijken en meewerken in je Autorespond-omgeving: contacten opzoeken, campagnes voorbereiden, automatiseringen controleren. Dat is ontzettend handig, maar je CRM staat vol met persoonsgegevens van jouw klanten. Zodra je AI-assistent meekijkt, gaan die gegevens naar de servers van de AI-leverancier, en daarmee ben jij volgens de AVG verantwoordelijk voor wat er gebeurt. Volg je de stappen hieronder rustig één voor één, dan regel je het netjes: eerst de juridische basis (stap 1 t/m 3), dan de technische inrichting met beperkte rechten (stap 4 t/m 7), en tot slot je AVG-administratie (stap 8 t/m 10).

*De MCP-koppeling in Autorespond is gebaseerd op **FluentCRM**, inbegrepen in je pakket. Lees de Engelse documentatie*

> **Belangrijk: jouw verantwoordelijkheid, geen juridisch advies.** Deze handleiding helpt je op weg, maar is algemene informatie en geen juridisch advies. Jij bent en blijft als ondernemer zelf verantwoordelijk voor het naleven van de AVG en andere wet- en regelgeving binnen jouw eigen situatie. Doe daarom altijd je eigen onderzoek: lees de actuele voorwaarden van je AI-leverancier, raadpleeg de Autoriteit Persoonsgegevens en schakel bij twijfel een jurist of privacy-adviseur in, zeker als je met gevoelige gegevens werkt. Autorespond aanvaardt geen aansprakelijkheid voor de manier waarop je deze koppeling gebruikt.

> **Welk AI-account gebruik je?** Leest je assistent gegevens van klanten, gebruik dan een zakelijk abonnement (Claude Team of Enterprise, ChatGPT Business of Enterprise). Daar worden je gegevens standaard niet gebruikt om de AI te trainen en sluit je een verwerkersovereenkomst. Een persoonlijk abonnement, gratis of betaald, heeft die overeenkomst niet. Gebruik je het voor werk zonder klantgegevens, zet dan in elk geval het

> trainen uit: in Claude onder Settings → Privacy, in ChatGPT onder Settings → Data controls. Een gratis account raden we af.

In het kort: de drie gouden regels

1. Gebruik **nooit** een gratis of persoonlijk AI-account voor klantgegevens. Alleen een zakelijk abonnement met een verwerkersovereenkomst.
2. Geef de AI een **eigen gebruiker met zo min mogelijk rechten**, nooit je beheerdersaccount.
3. Laat de AI **voorstellen doen, en verstuur zelf**. Geef het AI-account geen verzendrechten, tenzij je daar heel bewust voor kiest.

Deel A: de juridische basis

Stap 1: kies een zakelijk AI-abonnement

De AVG vereist dat je met iedere partij die persoonsgegevens voor jou verwerkt een **verwerkersovereenkomst** (Engels: DPA, Data Processing Agreement) hebt. Gratis en persoonlijke AI-abonnementen bieden die niet. Erger nog: die gebruiken je gesprekken standaard om het AI-model te trainen. De Autoriteit Persoonsgegevens waarschuwde eind 2025 nog expliciet voor datalekken doordat medewerkers klantgegevens in gratis chatbots plakken (AP-waarschuwing).

1. Kies een van deze opties:
   - **Claude** (Anthropic): een Claude for Work / Team-abonnement of de API. De verwerkersovereenkomst zit automatisch in de commerciële voorwaarden; Anthropic traint contractueel niet op jouw gegevens.
   - **ChatGPT** (OpenAI): een Team- of Enterprise-abonnement of de API. Onderteken de verwerkersovereenkomst via het DPA-portaal. OpenAI biedt op zakelijke abonnementen ook EU-dataopslag aan; vraag daar bij het afsluiten naar.
2. Bewaar (een kopie van) de verwerkersovereenkomst in je administratie.
3. **Niet doen:** je privé-account “even” gebruiken. Claude Free/Pro/Max en ChatGPT Free/Plus trainen standaard op je gesprekken en hebben geen verwerkersovereenkomst.

Stap 2: controleer de privacy-instellingen van je AI-account

1. Controleer dat **model-training uit staat** voor jouw omgeving. Op zakelijke abonnementen is dit standaard zo geregeld; controleer het toch even in de instellingen van je werkruimte.
2. Zet functies als “gesprekken delen ter verbetering” uit.
3. Beperk wie in jouw AI-werkruimte de CRM-koppeling mag gebruiken: alleen medewerkers die met klantgegevens mógen werken.

Stap 3: bepaal wat de AI wel en niet mag zien

De AVG vraagt om **dataminimalisatie**: geef de AI alleen toegang tot wat nodig is voor het doel.

1. Schrijf in één zin op waarvoor je de koppeling gebruikt. Bijvoorbeeld: *“De AI-assistent helpt ons met het opzoeken van contactinformatie en het voorbereiden van campagneteksten.”*
2. Werk je met gevoelige gegevens, bijvoorbeeld gezondheidsnotities als coach of therapeut? Zet die dan **niet** in velden waar de AI bij kan, of geef de AI helemaal geen toegang tot contacten. Bijzondere persoonsgegevens (gezondheid, geloofsovertuiging, enzovoort) horen niet via deze koppeling te lopen.
3. Beslis nu alvast welk profiel bij je past, dat maakt stap 5 makkelijker:
   - **Alleen meekijken** (aanbevolen om mee te starten): de AI kan lezen, jij doet alles wat verandert of verstuurt.
   - **Meewerken**: de AI mag ook contacten bijwerken en taggen, maar niet verwijderen en niet rechtstreeks mailen (let op: tags kunnen wél automatiseringen starten — zie stap 5).
   - **Volledig** (alleen voor gevorderden): de AI mag ook e-mails versturen. Lees eerst het onderdeel “Goed om te weten” onderaan dit artikel.

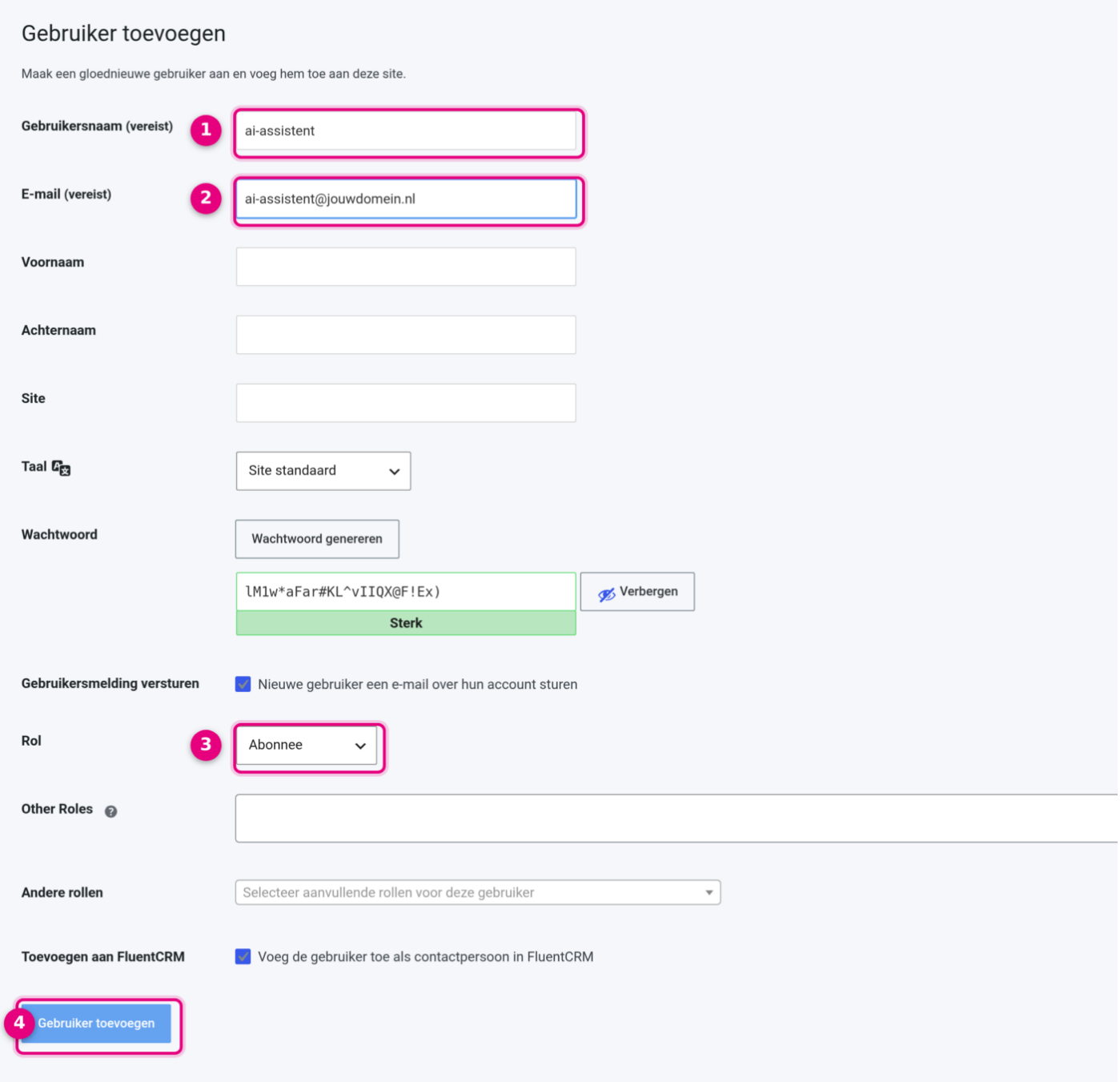
Deel B: de technische inrichting

Stap 4: maak een aparte gebruiker voor de AI

De koppeling werkt met de rechten van de gebruiker waarmee je hem aanmaakt. Gebruik je je eigen beheerdersaccount, dan kan de AI **alles**, inclusief campagnes versturen naar je hele lijst en contacten definitief verwijderen. Daarom maak je een aparte gebruiker met minimale rechten.

1. Ga in je beheeromgeving naar **Beheer → Gebruikers → Gebruiker toevoegen**.
2. Vul een gebruikersnaam in (bijvoorbeeld `ai-assistent`) en een eigen e-mailadres (bijvoorbeeld `ai-assistent@jouwdomein.nl`).

3. Kies bij Rol: **Abonnee**. Dat is de laagste rol en precies goed; de CRM-rechten regel je in stap 5 apart.
4. Klik op **Gebruiker toevoegen**.



Een aparte gebruiker voor de AI-assistent, met de laagste rol (Abonnee).

1. **Gebruikersnaam (vereist):** kies een herkenbare naam, bijvoorbeeld `ai-assistent`. Deze naam heb je in stap 7 weer nodig.
2. **E-mail (vereist):** een eigen adres voor dit account, bijvoorbeeld `ai-assistent@jouwdomein.nl`. Elk account heeft een uniek e-mailadres nodig.
3. **Rol:** kies **Abonnee**, de rol met de minste rechten.

4. **Gebruiker toevoegen:** hiermee maak je het account definitief aan.

Goed om te weten bij dit scherm: het vinkje **Gebruikersmelding versturen** mag uit, een AI-account hoeft geen welkomstmail te ontvangen. Zie je onderaan het vinkje **Toevoegen aan FluentCRM** (voeg de gebruiker toe als contactpersoon)? Zet dat uit, want dit hulpaccount hoort niet tussen je klantcontacten.

Stap 5: geef die gebruiker beperkte CRM-rechten

Het CRM heeft een eigen rechtensysteem dat losstaat van de gewone gebruikersrollen. Hier bepaal je heel precies wat de AI mag.

1. Ga naar **CRM & Emails → Instellingen** (het tandwiel rechtsboven) **→ CRM-managers**.
2. Klik op **Manager toevoegen** en vul het e-mailadres in van de gebruiker uit stap 4.
3. Vink onder Machtigingen alleen de rechten aan die bij je gekozen profiel horen (zie hieronder).
4. Klik op **Opslaan**.

Profiel “Alleen meekijken” (aanbevolen): vink alleen deze vier aan:

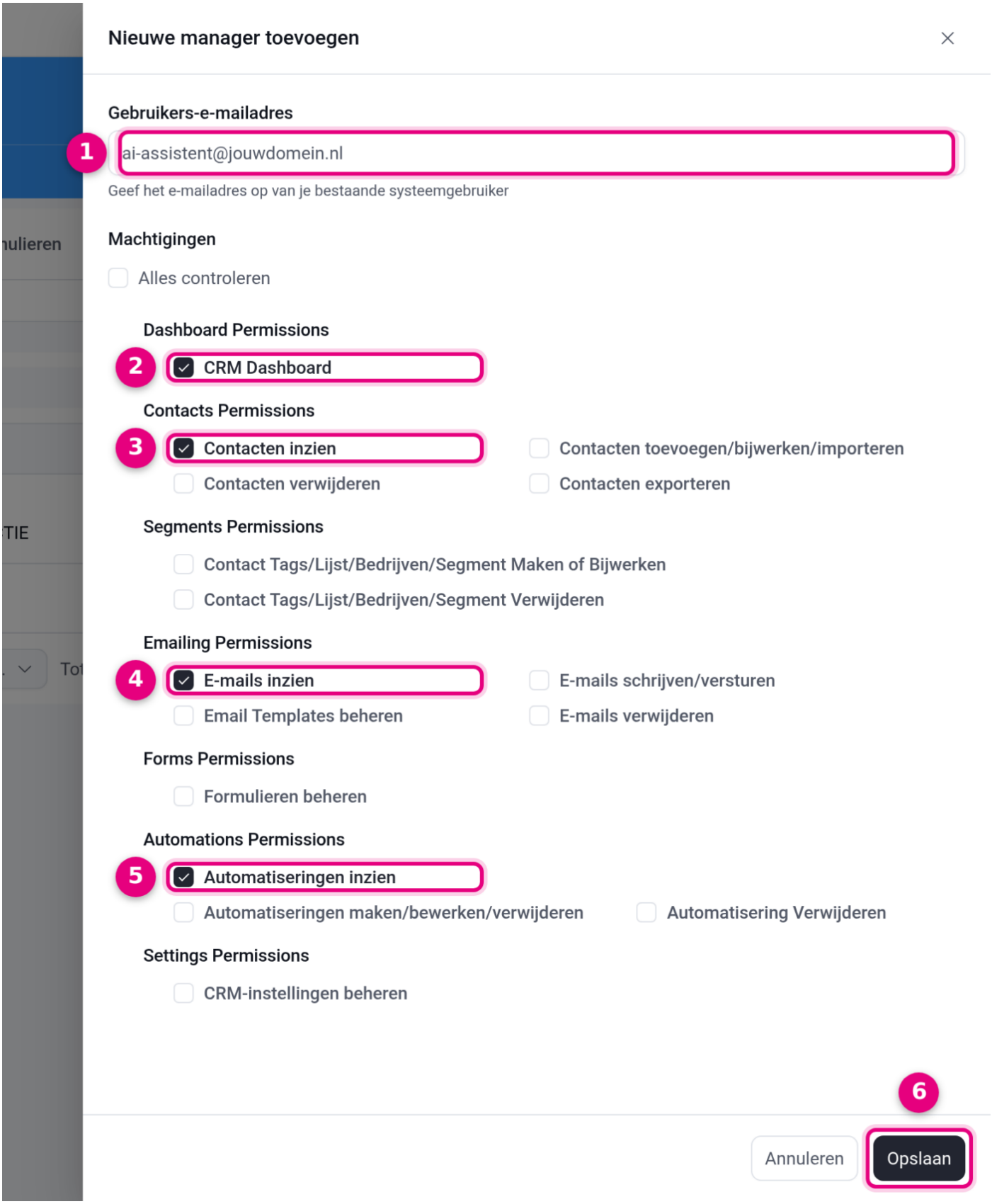
- CRM Dashboard
- Contacten inzien
- E-mails inzien
- Automatiseringen inzien

Profiel “Meewerken”: alles van hierboven, plus *Contacten toevoegen/bijwerken/importeren* en *Contact Tags/Lijst/Bedrijven/Segment Maken of Bijwerken*. Laat *Contacten verwijderen* en *E-mails schrijven/versturen* bewust uit.

> **Let op bij “Meewerken”:** heb je automatiseringen die starten zodra iemand een bepaalde tag of lijst krijgt? Dan kan de AI met dit profiel indirect tóch e-mails in gang zetten: een tag toekennen aan een contact start die automatisering gewoon, inclusief alle e-mails die erin zitten. Loop dus even je automatiseringen na voordat je de AI tags laat beheren — of blijf bij “Alleen meekijken”.

Profiel “Volledig”: alleen als je het risico kent (zie het onderdeel “Goed om te weten” onderaan), plus *E-mails schrijven/versturen*.

> **Waarom dit werkt:** elke functie van de koppeling controleert het bijbehorende CRM-recht op de server. Zonder “E-mails schrijven/versturen” kan de AI dus zelf geen mail versturen, wat de AI ook probeert (alleen via tag-gestarte automatiseringen kan er indirect mail uitgaan — zie het kader hierboven). Zonder “Contacten verwijderen” kan er niets verwijderd worden. Dit is je belangrijkste beveiliging.



Het venster “Nieuwe manager toevoegen”, ingevuld volgens het profiel “Alleen meekijken”.

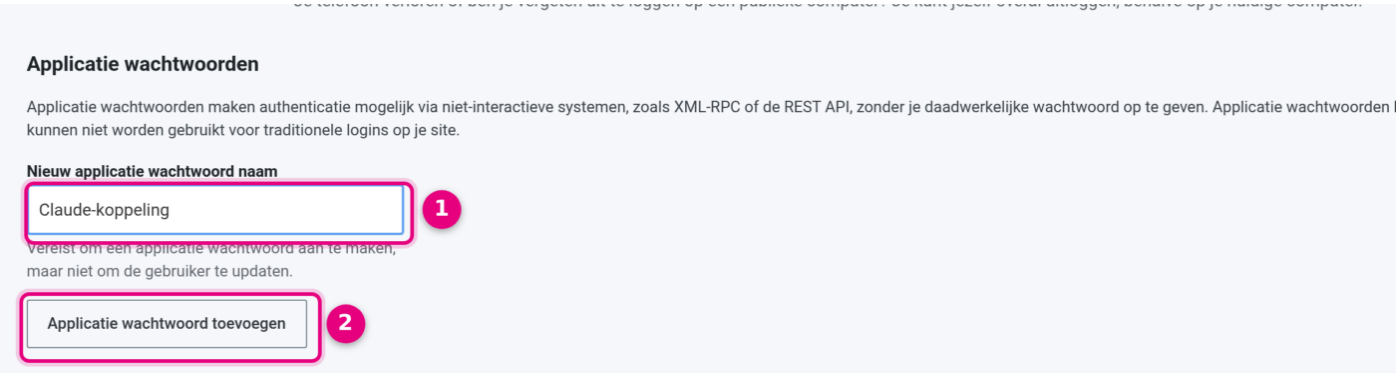
1. **Gebruikers-e-mailadres:** het e-mailadres van de AI-gebruiker die je in stap 4 hebt aangemaakt.
2. **CRM Dashboard:** de AI mag het dashboard met algemene cijfers bekijken.

3. **Contacten inzien:** alleen lézen van contacten. De vakjes voor toevoegen, verwijderen en exporteren laat je uit.
4. **E-mails inzien:** alleen lézen van campagnes en e-mails. “E-mails schrijven/versturen” laat je bewust uit.
5. **Automatiseringen inzien:** alleen lézen van automatiseringen, niet aanpassen of verwijderen.
6. **Opslaan:** hiermee ken je de rechten toe. Gebruik “Alles controleren” bovenaan dus níet, daarmee zou je juist alle rechten tegelijk aanzetten.

Stap 6: maak een applicatiewachtwoord aan

De AI logt niet in met een gewoon wachtwoord, maar met een **applicatiewachtwoord**: een aparte sleutel die je op elk moment kunt intrekken zonder dat er verder iets verandert.

1. Ga naar **Beheer → Gebruikers**, klik op de AI-gebruiker en scrol naar het kopje **Applicatie wachtwoorden**.
2. Geef het wachtwoord een herkenbare naam, bijvoorbeeld `Claude-koppeling`.
3. Klik op **Applicatie wachtwoord toevoegen** en **kopieer de code direct**, hij wordt maar één keer getoond.
4. Behandel deze code als een wachtwoord: niet mailen, niet in een gedeeld document zetten. Alleen invoeren in je AI-programma zelf (stap 7).



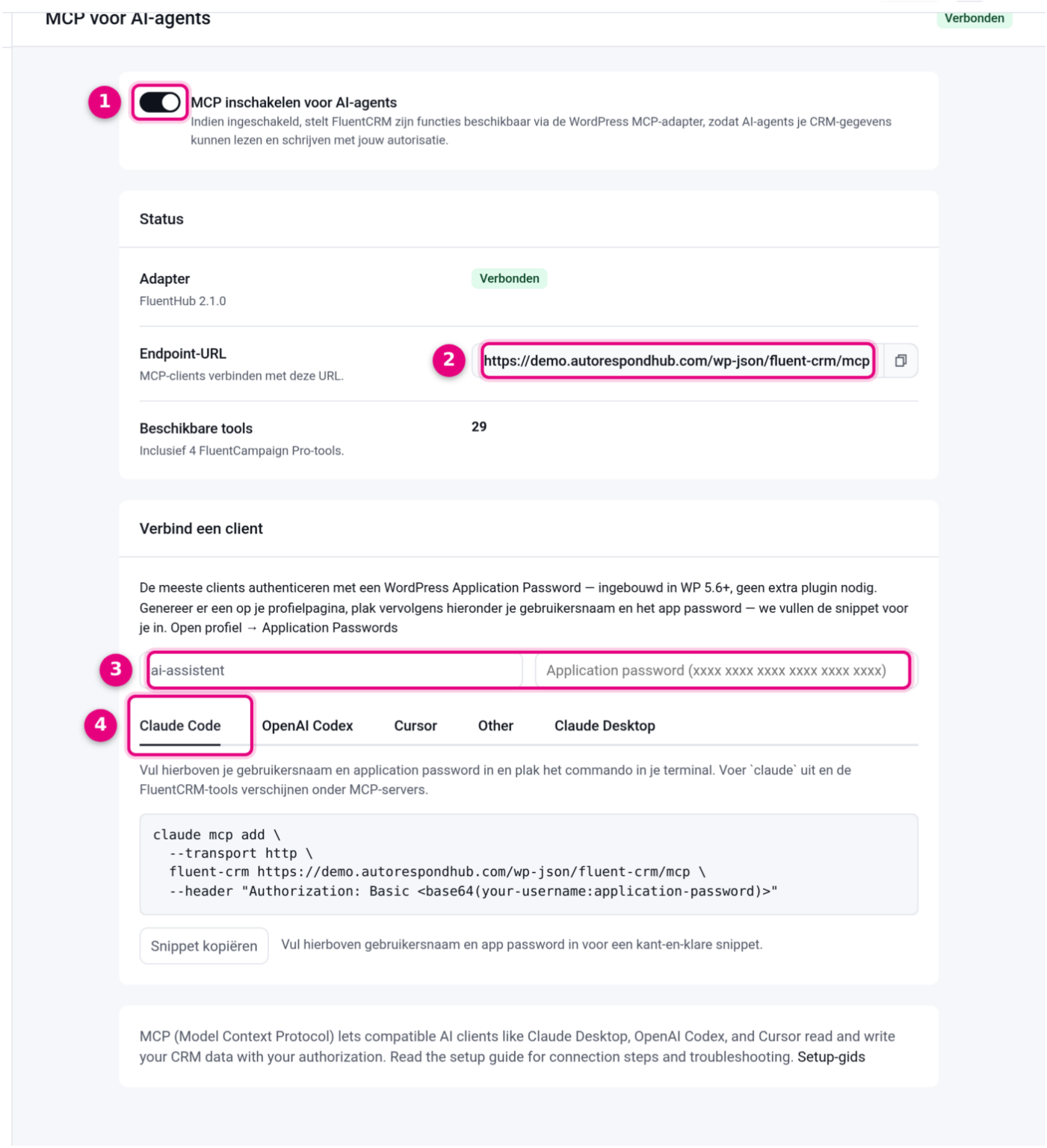
Het onderdeel “Applicatie wachtwoorden” op de profielpagina van de AI-gebruiker.

1. **Nieuw applicatie wachtwoord naam:** een herkenbare naam, zodat je later weet welke sleutel bij welke koppeling hoort.
2. **Applicatie wachtwoord toevoegen:** maakt de sleutel aan en toont de code eenmalig. Hierna verschijnt hier ook een lijst met bestaande sleutels, elk met een knop om hem in te trekken.

Stap 7: verbind je AI-assistent

1. Ga naar **CRM & Emails → Instellingen → AI-configuratie → MCP voor AI-agents**.

2. Controleer dat de schakelaar **MCP inschakelen voor AI-agents** aan staat. Onder Status zie je ook de **Endpoint-URL** van jouw koppeling; die eindigt op `/wp-json/fluent-crm/mcp`.
3. Vul bij **Verbind een client** de gebruikersnaam uit stap 4 en het applicatiewachtwoord uit stap 6 in.
4. Kies het tabblad van jouw AI-programma. Er staan kant-en-klare instructies klaar voor onder andere Claude Code, Claude Desktop en Cursor.
5. Kopieer de ingevulde snippet, volg de instructies voor jouw AI-programma en start het programma opnieuw op.
6. Test de verbinding met een onschuldige vraag, bijvoorbeeld: *“Hoeveel contacten staan er in mijn CRM?”*
7. Test ook meteen de beveiliging: vraag de AI iets wat hij níet mag, bijvoorbeeld *“verwijder testcontact X”*. Je hoort dan netjes “Permission denied”, en dat is precies de bedoeling.



De pagina “MCP voor AI-agents”: schakelaar, status en het onderdeel “Verbind een client”.

1. **MCP inschakelen voor AI-agents:** de hoofdschakelaar van de koppeling. Staat hij uit, dan werkt geen enkele AI-verbinding.
2. **Endpoint-URL:** het adres waarmee AI-programma’s verbinden. Op jouw omgeving staat hier het adres van je eigen site, eindigend op `/wp-json/fluent-crm/mcp`.
3. **Gebruikersnaam en applicatiewachtwoord:** vul hier de gegevens van de AI-gebruiker in; de snippet eronder wordt dan automatisch voor je ingevuld.

4. **Clientkeuze:** kies het tabblad van jouw AI-programma; de instructies en de snippet eronder passen zich daarop aan.

> **Tip:** ga je op vakantie of gebruik je de koppeling een tijd niet? Zet de schakelaar bovenaan deze pagina gerust even uit. Weer aanzetten is één klik.

Deel C: je AVG-administratie

Stap 8: vul je verwerkingsregister aan

Zet de nieuwe verwerking in je register van verwerkingsactiviteiten (artikel 30 AVG). Je mag deze voorbeeldregel overnemen en aanpassen:

Onderdeel	Invulling
Verwerkingsactiviteit	AI-assistentie bij klantbeheer en marketing (koppeling AI-assistent aan CRM)
Doel	Ondersteuning bij het opzoeken van klantinformatie en het voorbereiden van campagnes
Categorieën betrokkenen	Klanten, nieuwsbriefabonnees, leads
Categorieën gegevens	Naam, e-mailadres, tags/lijsten, campagne-interactie (géén bijzondere persoonsgegevens)
Ontvangers/verwerkers	[AI-leverancier, bijv. Anthropic], verwerkersovereenkomst d.d. [datum]
Doorgifte buiten EU	VS, op basis van standaardcontractbepalingen (SCC’s) in de verwerkersovereenkomst
Bewaartermijn	Gesprekken bij AI-leverancier: [30 dagen / conform contract]
Beveiliging	Aparte gebruiker met minimale rechten, intrekbaar applicatiewachtwoord, geen verzend- of verwijderrechten

Stap 9: werk je privacyverklaring bij

Voeg een alinea toe aan je privacyverklaring. Voorbeeldtekst die je mag overnemen:

> **Gebruik van AI-hulpmiddelen.** Voor het beheren van onze klantrelaties en het voorbereiden van onze e-mails maken wij gebruik van een AI-assistent van [leverancier, bijv. Anthropic]. Daarbij kunnen beperkte klantgegevens (zoals naam en e-mailadres) worden verwerkt op servers van deze leverancier, mogelijk in de Verenigde Staten. Wij hebben hiervoor een verwerkersovereenkomst gesloten met standaardcontractbepalingen; de leverancier gebruikt deze gegevens niet voor het trainen van AI-modellen. Vragen? Neem contact met ons op via [e-mailadres].

Stap 10: leg je afweging vast (pre-DPIA) en instrueer je team

1. **Korte risicoafweging (pre-DPIA).** Beantwoord voor jezelf schriftelijk, een half A4 is genoeg:
   - Welke gegevens kan de AI zien, en is dat het minimum voor mijn doel?
   - Verwerk ik gevoelige gegevens (gezondheid, kwetsbare groepen)? Zo ja: doe een volledige DPIA of laat je adviseren. De Autoriteit Persoonsgegevens beschouwt AI als “innovatieve technologie”, waardoor een DPIA al snel verplicht is.
   - Wat is het ergste dat er mis kan gaan, en welke maatregel dekt dat af?

   Gebruik als leidraad het Hulpmiddel generatieve AI en de AVG van de Autoriteit Persoonsgegevens (juli 2026).
2. **Instructie voor je team.** Dit dekt meteen de AI-geletterdheidsplicht uit de AI-verordening, die vanaf 2 augustus 2026 wordt gehandhaafd. Voorbeeldtekst vind je hieronder.
3. **Datalek-procedure.** Spreek af: gaat er tóch iets mis (bijvoorbeeld klantgegevens in een verkeerd of privé AI-account geplakt, of een applicatiewachtwoord gelekt), behandel het dan als mogelijk datalek. Trek het applicatiewachtwoord direct in (Beheer → Gebruikers → AI-gebruiker → Applicatie wachtwoorden → Intrekken), leg vast wat er is gebeurd, en beoordeel binnen 72 uur of melding bij de Autoriteit Persoonsgegevens nodig is.

> **Werkafspraken AI-assistent**
>
> - We gebruiken alleen het zakelijke AI-account van de zaak, nooit privé-accounts.
> - De AI mag meekijken en voorstellen doen; versturen, verwijderen en publiceren doen wij altijd zelf, na eigen controle.
> - Geen gezondheidsgegevens of andere gevoelige informatie aan de AI voorleggen.

> - Controleer AI-antwoorden altijd voordat je er iets mee doet richting een klant, want AI kan zich vergissen.
> - Twijfel of iets mag? Eerst overleggen met [naam].

Goed om te weten: wat kan er misgaan, en hoe heb je het afgedekt?

Risico	Hoe je het afdekt
De AI verstuurt ongevraagd een mailing naar je hele lijst	Geef het AI-account niet het recht “E-mails schrijven/versturen”. Zonder dat recht weigert de server elke verzendpoging.
De AI verwijdert contacten (definitief, inclusief e-mailgeschiedenis)	Geef niet het recht “Contacten verwijderen”.
Klantgegevens belanden bij de AI-leverancier	Dat is inherent aan de koppeling. Daarom: zakelijk abonnement, verwerkersovereenkomst en dataminimalisatie (deel A).
Iemand vindt je applicatiewachtwoord	Het is per direct intrekbaar en werkt alleen voor deze koppeling; je gewone wachtwoord blijft onaangetast.
De AI “verzint” iets of volgt verborgen instructies in een contactveld	Houd de mens in de lus: de AI stelt voor, jij controleert en voert uit. Start met het profiel “Alleen meekijken”.

Kies je toch voor het profiel “Volledig” (met verzendrechten)? Weet dan dat de AI daarmee zelfstandig e-mails en complete campagnes kan versturen, zonder extra bevestiging van de server. Sommige AI-programma’s vragen zelf om bevestiging bij zulke acties, maar daar kun je niet blind op vertrouwen. Ons advies: laat verzendrechten uit, en breid de rechten van het AI-account pas uit als je een paar weken prettig en foutloos met de koppeling werkt. Zelfs dan geldt: blijf elke verzendopdracht zelf nakijken.

Gerelateerde artikelen

- Je AI-assistent koppelen aan Autorespond: alle koppelingen op een rij
- Je kennisbank koppelen aan je AI-assistent (BetterDocs MCP)
- Je projecten en taken koppelen aan je AI-assistent (FluentBoards MCP)
- Twee-factor-authenticatie (2FA) aanzetten voor je beheeromgeving

- Uitgaande webhook naar Zapier instellen
- Uitgaande webhook naar Make instellen
- Automatisering triggers instellen

Al je e-mailmarketing, automatiseringen en klantbeheer op één Nederlands platform, met persoonlijke support die met je meedenkt? Dat is Autorespond.

Ontdek Autorespond →