Mail van Microsoft koppelen

De app registreren bij Microsoft, mailboxen en gedeelde postbussen koppelen, overnemen en Outlook-categorieën. Dezelfde teksten staan in het Helpcentrum van TrevantAI.

Waar gaat dit over?

Met de mailkoppeling worden bijlagen (en desgewenst de mails zelf) uit een mailbox vanzelf een bron in TrevantAI. Mailboxen van Microsoft (Microsoft 365 van een werk of school, Outlook.com en Hotmail) koppelt men niet met een wachtwoord, maar door zich aan te melden bij Microsoft zelf. TrevantAI krijgt dan een aanmeldsleutel die **alleen lezen** toestaat: het verzendt, verplaatst en verwijdert niets, en mails blijven ongelezen.

Deze handleiding is voor de beheerder én voor de gebruikers:

- **De beheerder** registreert eenmalig een app bij Microsoft (ongeveer tien minuten) en stelt die in TrevantAI in.
- **De gebruikers** koppelen daarna hun eigen mailbox en, als ze daar in Outlook al bij mogen, een gedeelde postbus, bijvoorbeeld voor facturen.

In Single-user is de gebruiker zelf de beheerder.

Wat er nodig is

- Een account waarmee men in **Microsoft Entra** (entra.microsoft.com) een app mag registreren. In een organisatie is dat meestal de beheerder van Microsoft 365 (de rol *Application Developer* of hoger). Voor *Grant admin consent* is een beheerder met de rol *Cloud Application Administrator* of *Global Administrator* nodig.
- Het adres waarop TrevantAI in de browser wordt geopend (bijvoorbeeld `https://trevantai.bedrijf.nl:3443`). TrevantAI toont het bij Beheer om te kopiëren.
- Voor privé-accounts (Outlook.com, Hotmail) zonder organisatie: een eigen (gratis) Azure-account om de app te registreren. Een centrale app van TrevantAI, zodat dat niet meer nodig is, volgt later.

TrevantAI levert geen eigen sleutels mee en bewaart geen geheim van de app: de app is een *openbare client* met een extra controlecode per aanmelding (PKCE). Een geheim zou na hoogstens twee jaar verlopen, en dan zou elke koppeling ineens stoppen.

Stap 1: de app registreren in Microsoft Entra

De namen hieronder staan in het Engels, zoals Microsoft Entra ze standaard toont. Staat Entra in een andere taal, dan heten de knoppen anders; de volgorde is dezelfde.

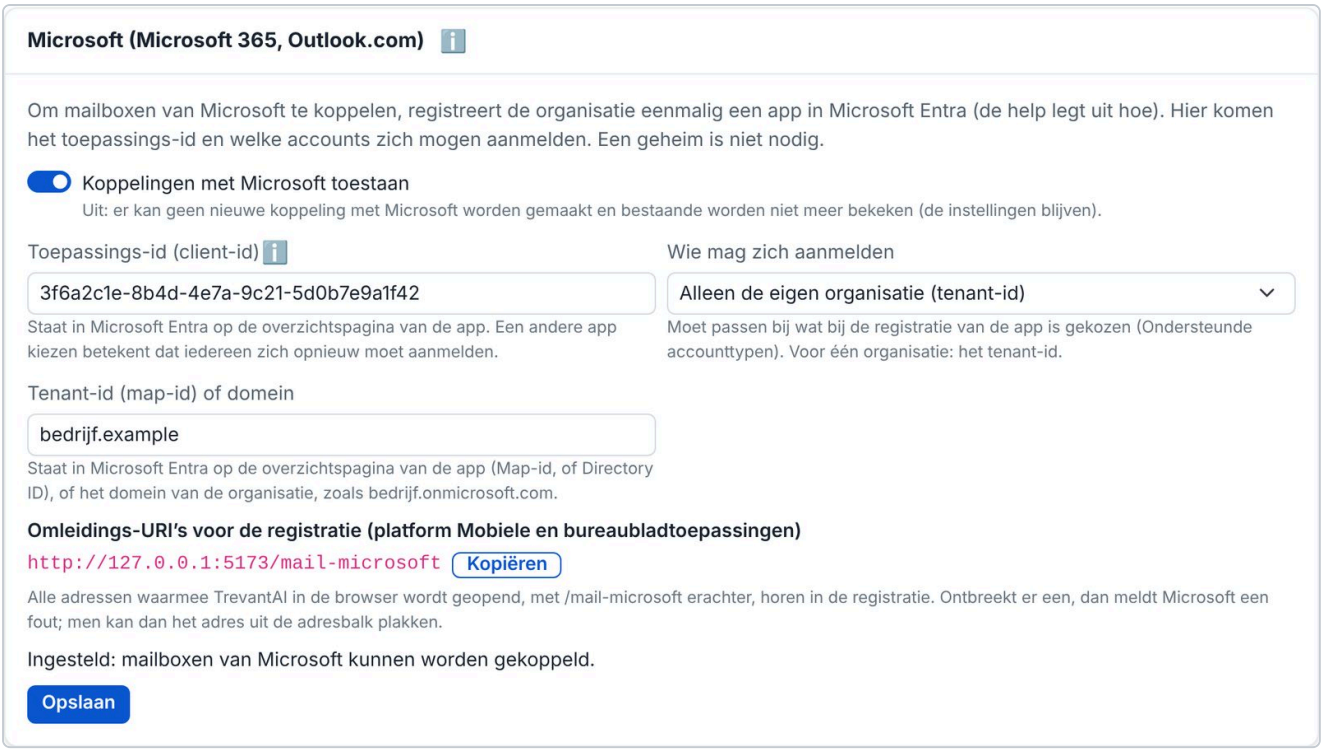
1. Ga naar **entra.microsoft.com** en meld u aan als beheerder. Kies links *Identity* > *Applications* > *App registrations* en dan **New registration**.
2. **Name**: bijvoorbeeld `TrevantAI`. Gebruikers zien deze naam bij het aanmelden.
3. **Supported account types**:

    - alleen de eigen organisatie: *Accounts in this organizational directory only* (aanbevolen);
    - ook andere organisaties: *Accounts in any organizational directory*;
    - ook privé-accounts (Outlook.com, Hotmail): *Accounts in any organizational directory and personal Microsoft accounts*.
4. **Redirect URI**: kies het platform **Public client/native (mobile & desktop)** en vul het adres in dat TrevantAI onder Beheer > Geplande taken > E-mail toont. Het eindigt altijd op `/mail-microsoft`. Kies dan **Register**.
5. Op de pagina **Overview** staan de **Application (client) ID** en de **Directory (tenant) ID**. Die twee komen in TrevantAI (stap 2).
6. Bij **Authentication**: voeg de andere adressen toe waarmee TrevantAI in de browser wordt geopend (een tweede naam, een IP-adres, `http://localhost:…` op de TrevantAI-computer zelf), elk met `/mail-microsoft` erachter. Laat *Allow public client flows* op *No* staan; dat is niet nodig.
7. Bij **API permissions**: *Add a permission* > *Microsoft Graph* > *Delegated permissions*, en vink aan:
    - `Mail.Read` (mail lezen);
    - `User.Read` (naam en adres van het account);
    - `offline_access` (aangemeld blijven, zodat TrevantAI elk kwartier vanzelf kan kijken);
    - `Mail.Read.Shared` (mail lezen in gedeelde postbussen; alleen nodig als gebruikers een gedeelde postbus koppelen). Kies daarna **Grant admin consent for …**. Dan hoeft niet elke gebruiker zelf in te stemmen, en werkt het ook als gebruikers dat in de organisatie niet mogen.
8. Bij **Certificates & secrets** hoeft niets: TrevantAI gebruikt geen geheim.

Vraag geen andere rechten aan. TrevantAI vraagt bij het aanmelden alleen wat hierboven staat; `Mail.Read.Shared` pas bij de eerste gedeelde postbus van een gebruiker.

Stap 2: de app instellen in TrevantAI

Onder **Beheer > Geplande taken > E-mail** staat de kaart **Microsoft**:



De kaart Microsoft onder Beheer > Geplande taken > E-mail

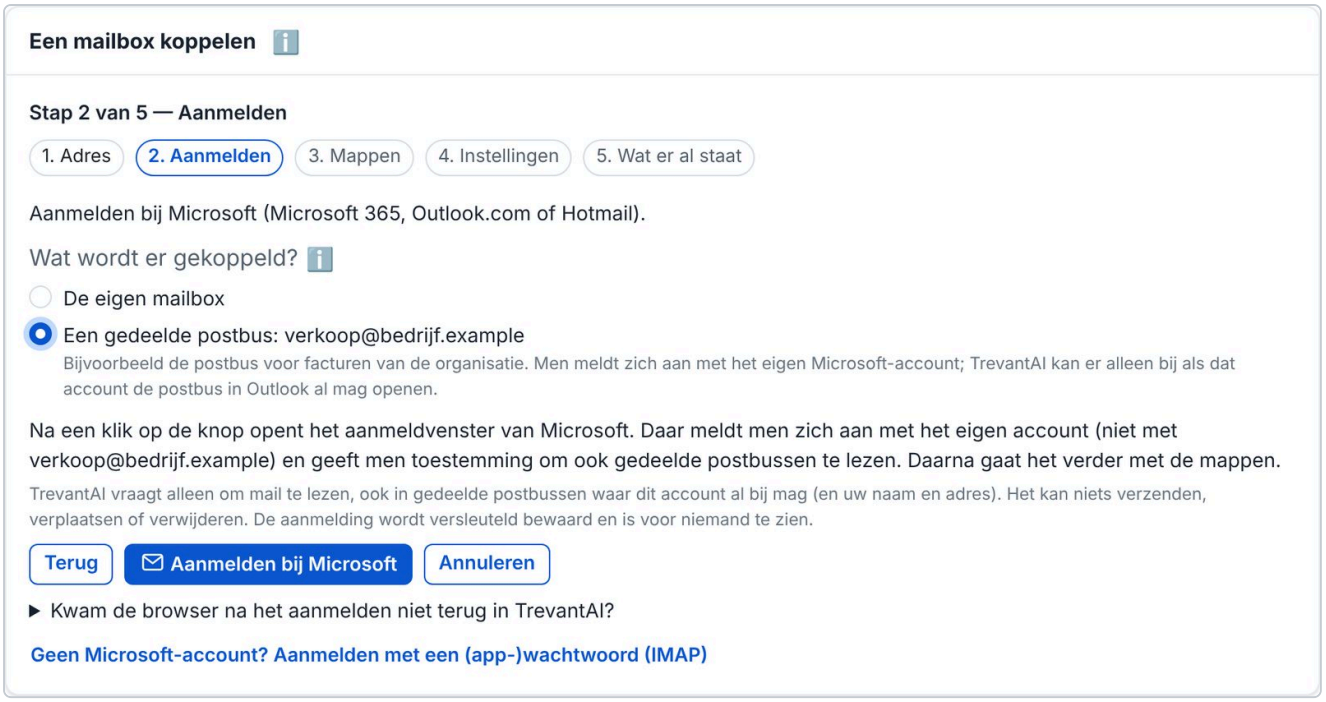
- **Koppelingen met Microsoft toestaan**: aan of uit, voor iedereen. Uit betekent geen nieuwe koppelingen, en bestaande worden niet meer bekeken (de instellingen blijven).
- **Toepassings-id (client-id)**: de *Application (client) ID* uit stap 1.
- **Wie mag zich aanmelden**: dezelfde keuze als bij *Supported account types*. Voor één organisatie: het tenant-id (*Directory (tenant) ID*) of het domein, zoals `bedrijf.onmicrosoft.com`.
- **Omleidings-URI's**: de adressen om in de registratie te zetten, met een knop om te kopiëren. Daaronder staat het adres dat deze browser nu gebruikt.

Kies **Opslaan**. Een ander toepassings-id of een andere tenant betekent later dat iedereen zich opnieuw moet aanmelden.

Een mailbox koppelen

Op het tabblad **Bronnen > Bronnen verkennen & toevoegen > E-mail** kiest men **Mailbox koppelen**. De wizard heeft vijf stappen: adres, aanmelden, mappen, instellingen en wat er al staat.

Herkent TrevantAI een adres van Microsoft, dan volgt *Aanmelden bij Microsoft*; bij een eigen domein kiest men zelf *Een Microsoft-account? Aanmelden bij Microsoft*. Bij stap 2 kiest men wat er gekoppeld wordt: **de eigen mailbox** of **een gedeelde postbus**.



Stap 2 van de wizard: de eigen mailbox of een gedeelde postbus

Na een klik op **Aanmelden bij Microsoft** opent het aanmeldvenster van Microsoft. Men meldt zich aan (met de tweede stap die de organisatie vraagt) en geeft toestemming. Daarna komt de browser vanzelf terug in TrevantAI, bij het kiezen van de mappen.

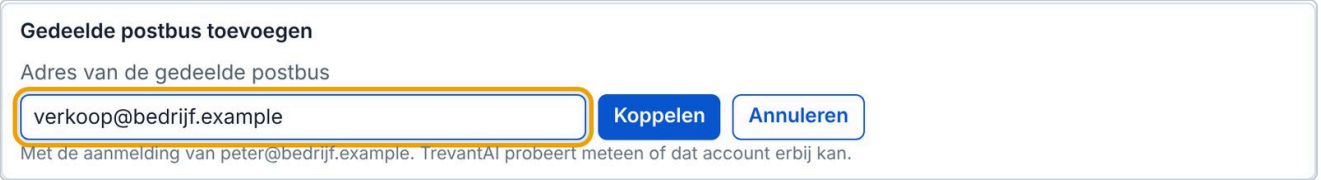
Komt de browser niet terug? Werkt men op een andere computer of via een adres dat niet in de registratie staat, dan toont de browser soms een foutpagina. Het adres in de adresbalk bevat dan nog de code. Dat adres kopiëren en in de wizard plakken bij *Kwam de browser na het aanmelden niet terug in TrevantAI?* rondt het aanmelden af (15 minuten geldig, één keer, alleen voor wie begon).

Een gedeelde postbus

Een gedeelde postbus van Microsoft 365, bijvoorbeeld `facturen@bedrijf.nl`, koppelt men met de **eigen** aanmelding. Wie de postbus in Outlook al mag openen, kan hem ook in TrevantAI koppelen; TrevantAI kan er niet meer dan dat account. Wie welke postbus mag openen, regelt de beheerder van Microsoft 365 (in het Exchange-beheercentrum: *Full Access* of *Read*), niet TrevantAI.

Er zijn twee manieren:

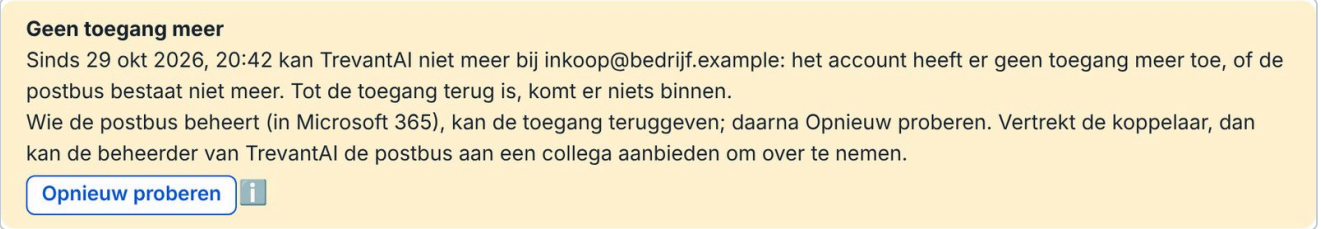
- in de wizard, met bij stap 2 **Een gedeelde postbus** (zie hierboven): men meldt zich aan met het eigen account, niet met het adres van de postbus;
- bij een mailbox van Microsoft die al gekoppeld is: **Gedeelde postbus toevoegen**, het adres invullen en **Koppelen**. Dan is geen nieuwe aanmelding nodig.



Gedeelde postbus toevoegen bij een gekoppelde mailbox

De eerste keer vraagt TrevantAI Microsoft om het recht `Mail.Read.Shared`; daarvoor meldt men zich één keer opnieuw aan. TrevantAI probeert meteen of het account bij de postbus kan. Lukt dat niet, dan wordt er niets bewaard en zegt TrevantAI waarom.

Geen toegang meer. Verliest het account later de toegang (of verdwijnt de postbus), dan staat bij de postbus *Geen toegang meer*, met een melding bij de envelop in de bovenbalk en per e-mail. De eigen mailbox gaat gewoon door. Na het teruggeven van de toegang: **Opnieuw proberen**. Er gaat niets verloren: de mails blijven in de postbus en TrevantAI haalt daarna alles in.



Geen toegang meer tot een gedeelde postbus

Eén aanmelding, meer postbussen

De eigen mailbox en elke gedeelde postbus zijn aparte koppelingen in de lijst, elk met eigen mappen, regels en Verzonden, maar ze delen **één aanmelding** bij Microsoft:

- **Opnieuw aanmelden** (bijvoorbeeld na een gewijzigd wachtwoord) geldt voor allemaal; TrevantAI noemt de andere postbussen erbij.
- Bij **Ontkoppelen** van de eigen mailbox vraagt TrevantAI of de gedeelde postbussen met dezelfde aanmelding ook ontkoppeld worden. Zonder vinkje blijven ze gekoppeld.



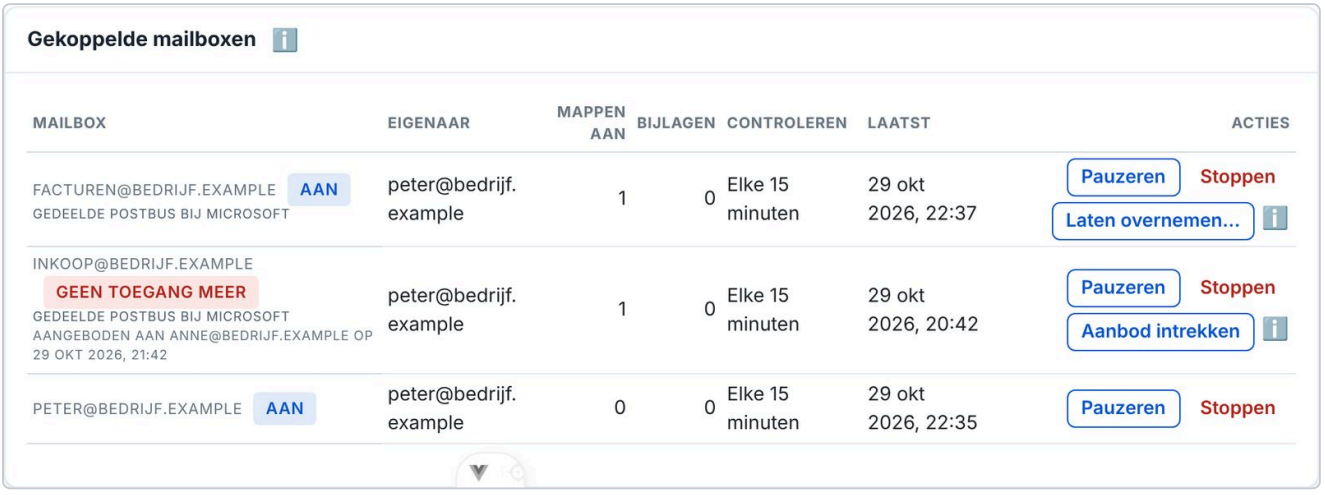
Ontkoppelen, met de vraag over de gedeelde postbussen

Alleen een gedeelde postbus koppelen, zonder de eigen mailbox, kan ook.

Overnemen als iemand vertrekt (Enterprise)

Een gedeelde postbus werkt met de aanmelding van wie hem koppelde. Vertrekt die, of raakt die de toegang kwijt, dan stopt de koppeling. In de Enterprise-editie kan de beheerder de koppeling daarom aan een collega aanbieden, ook al vóór iemand vertrekt.

In de lijst **Gekoppelde mailboxen** (Beheer > Geplande taken > E-mail) staat bij een gedeelde postbus **Laten overnemen…**, en bij een open aanbod **Aanbod intrekken**:



De gekoppelde mailboxen met Laten overnemen en Aanbod intrekken

Men kiest de collega en daarna **Laten overnemen…**:



Het venster Een gedeelde postbus laten overnemen

De collega krijgt een melding (ook per e-mail) en ziet het aanbod bovenaan het tabblad E-mail, met **Overnemen**:



Het aanbod om over te nemen, bij de collega

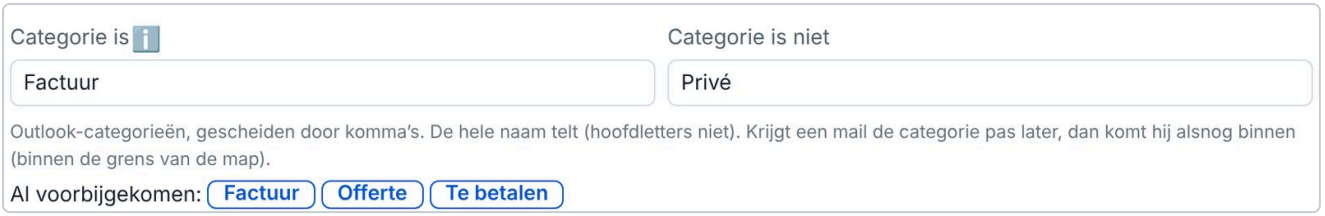
Overnemen gaat met de eigen aanmelding van de collega bij Microsoft; dat account moet bij de postbus kunnen. Daarna geldt:

- mappen, regels, Verzonden en wat TrevantAI van de postbus bijhield, gaan mee; er komt niets dubbel binnen;
- wat al binnenkwam (bronnen, e-mailgesprekken, kopjes), blijft van de vorige eigenaar, ook in teamprojecten;
- wat daarna binnenkomt, is van de overnemer;
- het teamproject en het documentsjabloon van een map blijven als de overnemer ze mag gebruiken; anders staat de map op geen project en *Vanzelf herkennen*, en zegt TrevantAI dat;
- de vorige eigenaar en de beheerder krijgen een melding; aanbieden, intrekken en overnemen staan in het beveiligingslogboek.

Alleen een gedeelde postbus kan worden overgenomen, niet iemands eigen mailbox.

Outlook-categorieën als regel

Veel mensen sorteren in Outlook met gekleurde **categorieën** in plaats van met mappen. Bij een mailbox van Microsoft hebben de regels van een map daarom ook **Categorie is** en **Categorie is niet**:



De regels Categorie is en Categorie is niet, met de categorieën die al voorbijkwamen

- Meer categorieën scheidt men met komma's; één ervan is genoeg.
- De hele naam telt (hoofdletters en accenten niet): *Factuur* past niet bij *Facturen 2026*.
- Onder de velden staan de categorieën die al voorbijkwamen; een klik zet er een bij *Categorie is*.
- Krijgt een mail de categorie pas later, bijvoorbeeld als men hem in Outlook sorteert, dan komt hij bij de volgende controle alsnog binnen (binnen de grens van de map).

Als het niet lukt

Wat men ziet	Wat er aan de hand is	Wat te doen
De beheerder heeft de koppeling met Microsoft nog niet ingesteld	Er is nog geen toepassings-id ingevuld.	Stap 1 en 2 van deze handleiding.
Dit terugadres staat niet in de registratie bij Microsoft (AADSTS50011)	Het adres van TrevantAI in de browser staat niet bij *Redirect URI*.	Het adres (met `/mail-microsoft`) toevoegen bij *Authentication*, of het adres uit de adresbalk plakken.
Een beheerder van uw organisatie moet eerst toestemming geven (AADSTS65001, AADSTS90094)	Gebruikers mogen in de organisatie zelf geen toestemming geven.	*Grant admin consent* bij *API permissions* (stap 1, punt 7).
Microsoft kent deze app niet (AADSTS700016)	Verkeerd toepassings-id, of een andere tenant dan waar de app staat.	Toepassings-id en *Wie mag zich aanmelden* nakijken.
aanmelden mislukt bij een mailbox	Wachtwoord gewijzigd, toestemming ingetrokken, account uitgeschakeld, of een ander toepassings-id.	*Opnieuw aanmelden*, met hetzelfde account als eerst.
Geen toegang meer bij een gedeelde postbus	Het account mag de postbus niet meer openen, of hij bestaat niet meer.	Toegang laten teruggeven in Microsoft 365, dan *Opnieuw proberen*; of (Enterprise) laten overnemen.
Een gedeelde postbus kan alleen bij een werk- of schoolaccount	De registratie is alleen voor persoonlijke accounts.	Een registratie voor werk- of schoolaccounts.

Wat men ziet	Wat er aan de hand is	Wat te doen
niet bereikbaar	Microsoft of het internet hapert.	Niets: TrevantAI probeert het vanzelf opnieuw en haalt daarna alles in.

Veiligheid en privacy

- TrevantAI vraagt alleen leesrechten en kan niets verzenden, verplaatsen of verwijderen.
- De aanmeldsleutel wordt versleuteld bewaard op de TrevantAI-computer (met `GEHEIM_SLEUTEL`), is voor niemand te zien, ook niet voor de beheerder, en gaat nooit mee in een projectbestand of export.
- *Ontkoppelen* wist de aanmelding in TrevantAI. Wie de toestemming ook bij Microsoft wil intrekken, doet dat bij het eigen Microsoft-account (bij de apps met toegang).
- Wordt het account van een gebruiker bij Microsoft uitgeschakeld, dan vervalt ook de toegang van TrevantAI.
- In mails en bijlagen staan vaak persoonsgegevens van anderen. Per map bepaalt de gebruiker wat er binnenkomt; voor wat er daarna mee gebeurt, gelden dezelfde regels als voor andere bronnen.