// deel 1 · per taak

Mag dit in ChatGPT?

Loop de vragen van boven naar beneden voordat je iets in een AI-tool zet. Bij de eerste vraag die van toepassing is, heb je je antwoord.

Je wilt iets in een AI-tool invoeren

1 Zitten er gegevens in die niet openbaar zijn?
Namen of gegevens van klanten en medewerkers, prijzen, offertes, tekeningen, contracten, cijfers.

nee → **Route 1 mag: elke tool**
Een algemene vraag, een openbare tekst, een eerste opzet. Ook een gratis versie is dan prima.

ja

2 Kun je de vraag ook stellen zonder die gegevens?
Vaak heb je alleen de kern nodig.

ja → **Doe dat: route 1 mag**
Vraag "hoe reageer ik op een klant die te laat betaalt?" in plaats van de mail van die klant te plakken. Hele documenten anonimiseren is veel werk en gaat snel mis.

nee

3 Heb je met een klant afgesproken dat gegevens binnen blijven?
Een NDA, een geheimhoudingsclausule of inkoopvoorwaarden over clouddiensten.

ja → **Lees eerst de afspraak**
Sluit die elke externe dienst uit, dan kan alleen route 4: een model op je eigen server. Mag het met afspraken, dan route 3. Twijfel je, dan niet met AI.

nee

4 Werk je in een zakelijke versie met verwerkersovereenkomst?
Daar staat training standaard uit. Check of je echt in het bedrijfsaccount zit.

nee → **Stop: niet invoeren**
Een gratis of privé-abonnement (ook Plus, Pro of Max) heeft geen verwerkersovereenkomst. AI gebeurd met persoonsgegevens? Mogelijk een datalek: vastleggen, en bij risico binnen 72 uur melden bij de AP.

ja: route 2, tenzij...

5 Gevoelige persoonsgegevens of je kroonjuwelen?
Gezondheid en verzuim, BSN, personeelsdossiers; rekenregels, recepturen, broncode, strategische plannen.

ja → **Route 3 of 4**
Een eigen omgeving in de EU met vastgelegde toegang en bewaartermijn, of een model op je eigen server. Voer alleen in wat nodig is.

nee

6 Moet AI dit elke dag doen, gekoppeld aan je systemen?
ERP, CRM, mailbox, dossiers: dan is het geen losse vraag meer maar een proces.

ja → **Route 3: eigen omgeving**
Een AI-agent die in je eigen EU-omgeving draait en met je systemen werkt. Kopiëren en plakken in een chat is dan foutgevoelig en niet te controleren.

nee

Route 2: de standaardroute
Een zakelijk account met verwerkersovereenkomst. Verdedigbaar, niet risicoloos: alleen met een AI-beleid, collega's die weten wat wel en niet mag, en geen feedbackknoppen bij gevoelige gesprekken.

Bij elke route: AI levert een concept. Jij controleert het en blijft verantwoordelijk voor wat er de deur uitgaat, zeker bij cijfers, prijzen en afspraken met klanten.

// deel 2 · voor je bedrijf

Welke omgeving richt je in?

Deel 1 loop je per taak af. Hier bepaal je één keer welke routes je bedrijf beschikbaar maakt. De meeste bedrijven hebben route 2 nodig, en voor een deel van het werk route 3 of 4.

1 Werk je met Microsoft 365 of Google Workspace?

ja → **Begin met route 2 in dat pakket**
Copilot of Gemini, onder het contract dat je al hebt. Anders: ChatGPT Business/Enterprise of Claude Team/Enterprise (Team kan vanaf 2 gebruikers).

daarna

2 Werk je vaak onder NDA of met kroonjuwelen?
Tekeningen van klanten, rekenregels, recepturen, personeelsdossiers.

ja → **Regel ook route 3 of 4**
Leg vast welk werk waar hoort, zodat niemand per geval hoeft te twijfelen.

daarna

3 Wil je AI koppelen aan je eigen systemen?
ERP, CRM, mailbox, planning.

ja → **Route 3: een eigen omgeving**
Model en automatisering in een EU-regio, met vastgelegde toegang, logging en bewaartermijnen.

daarna

4 Mag het niet bij een Amerikaanse partij terechtkomen?

ja → **Route 4, of een Europese aanbieder**
Een EU-regio bij een Amerikaans bedrijf (AWS, Google, Microsoft) valt nog onder de CLOUD Act. Alleen een Europese aanbieder of een model in eigen beheer haalt dat weg.

Wat je altijd regelt, welke route je ook kiest

- ☐ Verwerkersovereenkomst getekend en bewaard
- ☐ Iedereen werkt in het bedrijfsaccount, niet privé
- ☐ Een AI-beleid: welke tool voor welk werk, en wat nooit
- ☐ AI-geletterdheid voor wie ermee werkt (AI Act, art. 4)
- ☐ Geen feedbackknoppen (duimpjes) bij gevoelige gesprekken
- ☐ Afspraken met klanten (NDA's) naast je AI-gebruik gelegd
- ☐ Een DPIA als je AI inzet met gevoelige of veel persoonsgegevens
- ☐ Afgesproken wie een mogelijk datalek beoordeelt

De vier routes op een rij

Route	Voorbeelden	Waarvoor	Let op
1 · Gratis of privé	ChatGPT Free/Plus/Pro, Claude Free/Pro/Max, gratis Copilot of Gemini	Algemene vragen, openbare teksten. Nooit klant- of bedrijfsgegevens.	Invoer kan voor training worden gebruikt; geen verwerkersovereenkomst.
2 · Zakelijk account	ChatGPT Business/Enterprise, Claude Team/Enterprise, Copilot in M365, Gemini in Workspace	Het meeste dagelijkse werk, onder de voorwaarden uit deel 1.	Invoer meestal tot 30 dagen bewaard voor misbruikdetectie; Amerikaanse aanbieder.
3 · Eigen EU-omgeving	Model via een EU-regio (AWS Bedrock, Google Vertex, Azure) of een Europese aanbieder	Gevoelige gegevens, koppelingen met eigen systemen.	Vraagt inrichting en beheer. EU-regio bij een Amerikaans bedrijf: CLOUD Act blijft.
4 · Eigen server	Open model op eigen hardware, binnen je eigen netwerk	NDA's die externe diensten uitsluiten, je kroonjuwelen.	Hardware en beheer nodig; open modellen zijn minder krachtig.