



JOB AID · KB-AIDATA-001

# AI-veilig werken met persoonsgegevens



## WANNEER GEBRUIK JE DIT

- Je staat op het punt persoonsgegevens in een AI-tool te zetten.
- Je wilt met een AI-tool een brief opstellen, een tekst samenvatten of een antwoord formuleren, en er zitten persoonsgegevens in je invoer.
- Er zijn toch persoonsgegevens in een AI-tool terechtgekomen die er niet in hadden gemoeten. Ga dan direct naar "Twijfel of misgegaan".

## De routine Doe drie checks voordat je persoonsgegevens in een AI-tool zet.

### 1 CHECK Goedgekeurde tool

Alleen een tool die je organisatie heeft goedgekeurd. Geen gratis of openbare chatbot, tenzij goedgekeurd.

### 2 CHECK Toegestane gegevens

Alleen wat je nodig hebt, en alleen wat in die tool mag. Bij twijfel niet.

### 3 CHECK Toegestaan doel

Alleen voor een duidelijke, toegestane reden die past bij waarvoor de gegevens zijn verzameld.

## De beslisregel Kloppen alle drie? Ga verder. Klopt er één niet? Stop of schakel op.

✓ Alle drie · ga verder

✗ Eén niet · stop

### ✓ Wel

- ✓ Gebruik alleen een AI-tool die je organisatie heeft goedgekeurd voor persoonsgegevens.
- ✓ Voer alleen de gegevens in die je echt nodig hebt.
- ✓ Benoem de toegestane reden voordat je verder gaat.
- ✓ Meld het meteen via de route van je organisatie als er toch persoonsgegevens in een AI-tool terechtkomen.

### ✗ Niet

- ✗ Geen gratis of openbare chatbot voor persoonsgegevens, tenzij je organisatie die heeft goedgekeurd.
- ✗ Niet doorgaan met een niet-goedgekeurde tool, ook niet voor een concept en ook niet met de naam weggelaten.
- ✗ Niet doorgaan als je de reden voor het gebruik niet kunt benoemen.
- ✗ Niet afwachten bij een mogelijk datalek.

## Voorbeeld

Een collega wil de naam, het adres en het dossiernummer van een inwoner in een gratis chatbot zetten om een conceptbrief te maken. De chatbot staat niet op de goedgekeurde lijst.

Check 1 klopt al niet. Je stopt en gebruikt een goedgekeurde tool, of je werkt zonder de gegevens. "De naam weglaten" of "het is maar een concept" maakt dit niet goed: de tool is niet goedgekeurd.



## Twijfel of misgegaan

**Twijfel je bij een check?** Niet doen. Stop of schakel op via [\[escalatierroute\]](#).

**Toch misgegaan?** Behandel het als een mogelijk datalek en meld het meteen via [\[meldroute\]](#). Wacht niet af.

## Lokale waarden IN TE VULLEN BIJ KLANT-SETUP

Goedgekeurde AI-tools [\[goedgekeurde AI-tools\]](#)

Toegestane gegevenscategorieën [\[toegestane gegevenscategorieën\]](#)

Toegestane doelen [\[toegestane doelen\]](#)

Meldroute bij mogelijk datalek [\[meldroute\]](#)

Escalatieroute bij twijfel [\[escalatieroute\]](#)