

AI veilig en AVG-proof.

AI is handig, maar wat je erin typt gaat wel ergens heen. Deze gids legt in gewone taal uit wat je wel en niet deelt, hoe je met klantgegevens omgaat en waar je op let volgens de AVG. Geen juridisch verhaal, wel praktisch.

Als je iets in een AI-tool typt, verstuur je dat naar de servers van de aanbieder. Bij veel gratis diensten kan die informatie gebruikt worden om het model te trainen. Voor een blogtekst is dat geen probleem. Voor het dossier van een klant wel. De kern is simpel: bedenk voordat je iets plakt of het erg zou zijn als het naar buiten kwam.

DE GOUDEN REGEL

Zet niets in een AI-tool wat je niet ook op een ansichtkaart zou schrijven. Twijfel je? Haal de persoonlijke gegevens er eerst uit.

Wat je beter niet deelt

- Namen, adressen, telefoonnummers en e-mailadressen van klanten.
- Burgerservicenummers, kopieën van identiteitsbewijzen en medische gegevens.
- Wachtwoorden, inloggegevens en interne codes.
- Bedrijfsgeheimen, contracten en cijfers die niet naar buiten mogen.

Wat wel prima kan

- Algemene teksten, ideeën en voorbeelden zonder persoonlijke gegevens.
- Een klantvraag waar je eerst de naam en contactgegevens uit hebt gehaald.
- Openbare informatie, zoals een tekst die toch al op je website staat.

Anonimiseren in de praktijk

Wil je toch hulp bij een echte casus? Vervang de persoonlijke gegevens door algemene woorden. Maak van "Jan de Vries, Kerkstraat 1" gewoon "de klant". De AI kan je nog

steeds helpen met de tekst, zonder dat je iemands gegevens deelt. Dit kleine gewoontetje lost het grootste deel van de risico's op.

De AVG in het kort

De AVG is de Europese privacywet. Voor AI komt het op een paar dingen neer:

- **Doel.** Gebruik persoonsgegevens alleen waarvoor je ze hebt gekregen.
- **Zo min mogelijk.** Deel niet meer dan nodig is voor de taak.
- **Grip.** Je moet weten waar gegevens heen gaan. Bij een willekeurige gratis tool weet je dat vaak niet.
- **Afspraken.** Verwerkt een tool namens jou persoonsgegevens, dan hoort daar formeel een verwerkersovereenkomst bij.

Veiliger werken met AI

1. Gebruik waar mogelijk een zakelijke versie. Betaalde zakelijke abonnementen beloven meestal dat ze je invoer niet gebruiken om te trainen.
2. Zet de trainingsoptie uit als de tool dat toelaat.
3. Maak binnen je bedrijf één simpele afspraak over wat wel en niet mag. Een half A4 is genoeg.
4. Twijfel je over een specifieke situatie? Vraag het na. Beter één vraag te veel dan een datalek.

LET OP

Deze gids helpt je op weg maar is geen juridisch advies. Werk je met veel gevoelige gegevens, laat je situatie dan een keer goed bekijken. Wij denken graag mee over een veilige aanpak.