TRANSPARANT SAMENWERKEN

De 12 regels voor veilig AI-gebruik in jouw bedrijf

Een korte praktijkgids voor MKB-ondernemers en hun team. Lees in 15 minuten, hang op kantoor, deel met je collega's.

Waarom deze gids

AI staat in een jaar tijd op iedere werkvloer. ChatGPT, Claude, chatbots, agents, koppelingen. Iedereen probeert iets, weinigen weten waar de gevaren zitten.

Je hoeft geen techneut te zijn om je bedrijf veilig te houden. Je moet wel weten welke vuistregels gelden. Hieronder de 12 belangrijkste, in volgorde van impact.

Print uit en hang op. Of stuur door. Het kost je 15 minuten.

01. Geen klantdata in een gratis AI-tool

Op de gratis en consumer-plannen van ChatGPT (Free, Plus) traint OpenAI standaard mee op je gesprekken, tenzij je dat handmatig uitzet. Voor klantwerk: Team-plan of hoger.

Concrete actie: Check vandaag welk plan je gebruikt. Werk je met klantdata? Stap over op Team of Enterprise.

02. Anonimiseer voor je iets in een prompt plakt

Vervang namen door [KLANT_A], adressen door [ADRES], laat bedragen staan. Het antwoord wordt er niet slechter van, en je bent veilig.

Concrete actie: Maak een mini-checklist van wat je nooit plakt: BSN, salarisstroken, ondertekende contracten, klantenlijsten, wachtwoorden, API-keys.

03. Tweestapsverificatie (2FA) op elke AI-tool

Een gestolen wachtwoord opent je hele AI-geschiedenis met klantdata. 2FA is gratis en zet je in 30 seconden aan.

Concrete actie: Loop deze week alle AI-tools langs: ChatGPT, Claude, Copilot, Gemini, Apollo, Jasper. 2FA aan, klaar.

04. Verwerkersovereenkomst (DPA) tekenen

Onder de AVG ben je verplicht om een DPA af te sluiten met elke partij die persoonsgegevens voor je verwerkt. Ook OpenAI en Anthropic. Beide hebben een standaard-DPA klaarliggen.

Concrete actie: Download bij OpenAI en Anthropic de DPA, laat directie tekenen, sla op in je AVG-map.

05. Kies Team of Enterprise voor klantwerk, niet Free of Plus

Op Team en Enterprise wordt nooit op jouw data getraind, geldt sterke data-policy en is een DPA standaard. Bij gevoelige sectoren (zorg, juridisch, finance) is Microsoft Copilot 365 vaak nog veiliger omdat data in je eigen tenant blijft.

Concrete actie: Maak een tabel: welke teamleden gebruiken AI, welk plan zitten ze op, welk plan past bij hun werk.

06. Check elk kwartaal je privacy-instellingen

AI-leveranciers tonen geregeld opt-in pop-ups voor het delen van data of het meetrainen op gesprekken. Veel mensen klikken gedachteloos op ja.

Concrete actie: Zet in je agenda: kwartaal-check Settings van ChatGPT, Claude, Copilot. 10 minuten werk.

07. Breng schaduw-AI in beeld

In een MKB van 20 mensen draaien gemiddeld 8 tot 12 verschillende AI-tools, waarvan de directie er maar een paar kent. Marketing gebruikt Jasper, sales een Apollo-extensie, finance test een Excel-plug-in. In elk zit klantdata.

Concrete actie: Eens per kwartaal: vraag iedereen welke AI-tools ze gebruiken. Niet om af te straffen, om in beeld te krijgen.

08. Zet een dagelijkse kostenlimiet op API-keys

Wie zonder limiet werkt en een lekgekomen key heeft, kan in 24 uur duizenden euro's aan API-kosten oplopen. Dat is geen verzonnen scenario.

Concrete actie: In OpenAI en Anthropic dashboards: zet een soft limit en hard limit per maand. Voor MKB meestal voldoende: 50 tot 200 euro hard limit.

09. Vermeld op je website dat klanten met AI praten

Heb je een chatbot of AI-mailafhandelaar die met klanten communiceert? Dan moet je vermelden dat het een AI is. Vanaf augustus 2026 verplicht onder de EU AI Act.

Concrete actie: Voeg een korte zin toe bij chatbot-launch: "Je praat met een AI-assistent. Een mens neemt over als het nodig is."

10. Schrijf op wie je belt als er iets misgaat

Bij een datalek heb je 72 uur om te melden bij de Autoriteit Persoonsgegevens. Als je niet weet wie je belt, raak je waardevolle uren kwijt aan paniek.

Concrete actie: Maak een briefje: AVG-contact, IT-leverancier, juridisch adviseur, AI-leverancier (support-mail). Hang op kantoor of in je AVG-map.

11. Bel terug op het bekende nummer

Phishing in 2026 ziet er anders uit. AI schrijft mails zonder fouten, doet stemmen na via WhatsApp. Een belletje van "je manager" die om een spoed-overschrijving vraagt is geen sciencefiction meer.

Concrete actie: Spoed plus geld plus afwijkend verzoek: altijd dubbel checken via een nummer dat je al kende. Niet via het nummer in het bericht.

12. Train je team elk kwartaal

Eenmalig een training is onvoldoende. AI verandert maandelijks, en dat doen ook de risico's. Kort en herhaald werkt beter dan lang en eenmalig.

Concrete actie: Plan elk kwartaal 30 minuten: nieuwe risico's bespreken, 1 phishing-simulatie, 1 nieuwe vuistregel. Klaar.

Wat nu?

Niet alle 12 regels tegelijk. Begin bij de eerste drie:

- Welk plan gebruik je nu? Team of Free?
- Heb je een DPA met je AI-leverancier?
- Staat 2FA aan op alle accounts?

Daarna pak je elke maand er een paar bij. Binnen een kwartaal sta je voor.

Wil je dieper de stof in?

Op transparantsamenwerken.nl staat de complete AI-Security gids (30 minuten lezen, met checklist en incident-cases). Voor teams: een incompany-licentie waarbij je hele team toegang krijgt tot de kennisbank, vanaf 750 euro per jaar.

Vragen of feedback?

Mail Roy direct op roy@transparantsamenwerken.nl. Antwoord binnen 24 uur.