tico.

3 lagen voor AI met klantdata

Een praktische aanpak voor MKB-ondernemers

MKB-gids

Mei 2026

51% van NL-ondernemers vreest datalekken door AI. Slechts 7% weet hoe de regels echt zitten (Rijksoverheid + KVK, eind 2025). Deze gids dicht dat gat in drie concrete lagen.

Laag 1 — Voorkom dat AI op jouw data traint

De waarheid in één zin: het ligt niet aan de provider, het ligt aan welk abonnement je gebruikt.

Consumer-tier (ChatGPT Free of Plus, Claude Pro, Gemini-app): data wordt standaard gebruikt voor training. Anthropic zette die toggle in augustus 2025 zelfs default op aan, klein gedrukt onder een grote Accept-knop.

Business-tier (ChatGPT Team of Enterprise, Claude for Work, Microsoft 365 Copilot, Gemini for Workspace): training op klantdata is contractueel uitgesloten. Zwart-op-wit in de Commercial Terms en DPA's.

Tool	Training default	Waar zet je 'm uit
ChatGPT Free of Plus	Aan	Settings → Data Controls → "Improve the model" → uit
Claude Pro of Max	Aan sinds aug 2025	Privacy Settings → "Help improve Claude" → uit
Gemini-app	Aan	myactivity.google.com → Gemini Apps Activity → pauzeren
ChatGPT Team of Enterprise	Uit (contractueel)	Geen actie nodig
Claude for Work	Uit (contractueel)	Geen actie nodig
Microsoft 365 Copilot	Uit (contractueel)	Geen actie nodig
Gemini for Workspace	Uit (contractueel)	Geen actie nodig

Laag 2 — Werk veilig met klantdata

Niet alle business-tiers zijn gelijk. Voor MKB met klantdata uit gereguleerde sectoren (zorg, finance, juridisch) zijn er vier extra keuzes.

Soort werk	Bevat klantdata	Tier-eis
Marketing-teksten, eigen content	Nee	Consumer Pro of business
Klant-mails, offertes, contracten	Ja	Business verplicht, EU-residency aanbevolen
CRM-data, contracten, financieel	Ja, gevoelig	Business + EU Data Boundary + DPA-audit
Zorg, finance, juridisch	Ja, hoog-risico	Business + EU + sectorale audit + DPIA

Drie regels die werken naast de tier-keuze: één officieel AI-pakket voor het hele team (geen "iedereen eigen account"), schriftelijke werkinstructie van één pagina (wat mag wel, wat niet), en anonimiseer waar het kan (klantnaam vervangen door [KLANT], bedragen in ranges).

Laag 3 — Ondernemers-roadmap

Vijf stappen die je deze maand zet. Geen consultancy nodig.

01

AI-inventarisatie. Maak een lijst van alle AI-tools die je team gebruikt. Vraag het rond. Per tool drie vragen: welke tier, wie gebruikt het, op welke data. Eén uur werk.

02

Tier-keuze. Op basis van laag 2: welke business-tier rol je voor het hele team uit? Eén keuze. Geen versnipperde abonnementen.

03

Beleid op één pagina. Wat mag wel in AI. Wat niet. Wat te doen bij twijfel. Wie de eindverantwoordelijke is. Hoe nieuwe tools worden goedgekeurd. Waar het AI-register staat.

04

Training van mensen. Tools veranderen sneller dan policies. Mensen moeten weten waarom de regels er zijn, niet alleen wat ze zijn. Anders weten ze niet wanneer ze moeten escaleren.

05

Toezicht vanaf 2 augustus 2026. EU AI Act geldt vanaf die datum. Houd een AI-register bij (een notitie-app is genoeg). Markeer AI-gegenereerde content als AI. Klaar.

Wat WEL een echt risico is (en niet over training gaat)

- Credential theft. Group-IB vond in 2022-2023 ruim 101.000 met infostealer besmette devices met opgeslagen ChatGPT-credentials. Oplossing: MFA verplicht, geen wachtwoord-hergebruik.
- Cross-user lekken. De Redis-bug van maart 2023 toonde gesprekstitels van 1,2% ChatGPT Plus-gebruikers aan andere users. Klassiek software-incident.
- Shadow-IT. Samsung-engineers plakten broncode in consumer-ChatGPT zonder dat IT het wist. Oplossing: één officieel pakket plus monitoring.
- Prompt injection. AI-agents zijn meermaals misleid via verstopte instructies in e-mails of documenten. Oplossing: agents niet zonder review op klantdata loslaten.

Training is in 99% van de MKB-AI-incidenten niet het probleem. De mens en de configuratie wel.

Bronnen

Anthropic Privacy Center, Anthropic Consumer Terms update (28 aug 2025), OpenAI Enterprise privacy, Microsoft 365 Copilot privacy (Microsoft Learn), Google Workspace AI privacy, EDPB Opinion 28/2024, Autoriteit Persoonsgegevens "AP-visie op generatieve AI" (mei 2025), Rijksoverheid "AI-gebruik in het mkb" (sep 2025), KVK-onderzoek AI-wetgeving.

Over Tico.

Tico van Gerner helpt MKB-bedrijven met praktische software voor klantcontact, service en facturatie. Bij Aiden doet hij SAP CX-implementaties; daarnaast bouwt hij Fikst — maatwerk-software voor installatie-MKB.

Connect op LinkedIn → linkedin.com/in/ticovangerner