



AI Security

5 risico's die iedere B2B marketeer moet kennen

Waarom dit **belangrijk** is

AI maakt je marketing sneller en effectiever. Maar elke tool die jouw data verwerkt, brengt risico's mee. Niet omdat AI zo gevaarlijk is dat je het niet zou moeten gebruiken, maar omdat veel marketing- en salesteams simpelweg niet weten waar ze op moeten letten.

Dit zijn de vijf risico's die nu al spelen in jouw dagelijkse werk, en wat je er concreet aan kunt doen.

Wist je dat...

18% van alle medewerkers plakt bedrijfsdata in GenAI-tools, waarvan 50% gevoelige bedrijfsinformatie. 99% van de organisaties heeft al data blootgesteld die door AI gevonden kan worden. Bron: [LayerX Enterprise GenAI Security Report 2025](#) >

De 5 risico's voor marketing & sales professionals

1

Shadow AI in je team

Collega's gebruiken ChatGPT, Claude of andere AI-tools zonder dat IT of management dit weet of heeft goedgekeurd. Ze doen het niet met kwade bedoelingen, maar omdat het werkt en er geen veilig alternatief is aangeboden. Zolang er geen beleid is, is er ook geen zicht op welke data er gedeeld wordt, met welke tool, en onder welke voorwaarden.

Actie: Maak een lijst van goedgekeurde AI-tools en deel die actief. Geef je team een veilig alternatief, want verbieden werkt niet.

2

Klantdata in publieke AI-tools

Een campagnebriefing met klantgegevens, een CRM-export voor segmentatie of een leadlijst in een chatbot om teksten te personaliseren. Het lijkt handig, maar bij de gratis versie van ChatGPT staat "data gebruiken voor modeltraining" standaard aan. Jouw klantdata wordt zo trainingsmateriaal voor een publiek AI-model.

Actie: Verwerk nooit klantspecifieke data in niet-goedgekeurde tools. Gebruik altijd de betaalde, zakelijke versie met de juiste privacy-instellingen.

3

Geen controle op AI-output

AI hallucineert. Het verzint statistieken, fabriceert citaten en maakt claims die nergens op gebaseerd zijn, maar wel overtuigend klinken. Als die fouten in je content, offertes of salesgesprekken belanden, is de reputatieschade al gedaan voordat je het door hebt. En in de context van de EU AI Act: jij bent aansprakelijk voor wat je publiceert, ook als AI het heeft geschreven.

Actie: Een medewerker controleert altijd voor publicatie. Leg intern vast wie de eindcheck doet op AI-content, en maak dit onderdeel van je standaard werkproces.

4

Onduidelijkheid over aansprakelijkheid

AI-content kan fouten bevatten, misleidend zijn of auteursrechtelijk beschermd materiaal gebruiken. De vraag "wie is er verantwoordelijk?" is in veel marketing- en salesteams nog niet beantwoord. De EU AI Act maakt dit urgent: organisaties zijn verantwoordelijk voor de AI-systemen die ze inzetten, ook als de fout bij het model ligt.

Actie: Leg nu al intern vast wie eindverantwoordelijk is voor AI-gegenereerde content en communicatie. Dit is geen IT-vraag, dit is een managementvraag.

5

AVG- en AI Act-compliance

De EU AI Act is van kracht en de meeste verplichtingen gaan in op 2 augustus 2026. Voor marketing en sales betekent dit concreet: chatbots moeten zich kenbaar maken als AI, AI-gegenereerde content in risicovolle contexten moet worden gelabeld, en je hebt een verwerkersovereenkomst nodig met AI-leveranciers die persoonsgegevens verwerken. Veel organisaties weten dit nog niet, of hebben het nog niet geregeld. De deadline nadert sneller dan je denkt.

Actie: Check of je AI-leveranciers een verwerkersovereenkomst hebben getekend. Vraag je toolsleverancier of ze EU-datalocatie bieden. Controleer of je chatbot zich kenbaar maakt als AI.

Gratis of betaald: het verschil dat ertoe doet

Gratis versie	Betaalde versie
Data-opslag standaard AAN	Data-opslag uitzetten mogelijk (of standaard uit, zoals bij Claude)
Jouw input kan worden gebruikt voor modeltraining	SSO, admin controls en audit logs beschikbaar
Geen enterprise controls, geen AVG-garanties	AVG-compliance opties aanwezig
Geschikt voor privégebruik, niet voor bedrijfsdata	Controleer na elke upgrade: instellingen kunnen resetten

Quick checklist: doe dit vandaag

- ☐ ChatGPT: ga naar Settings > Data Controls en zet "model verbeteren voor iedereen" op UIT
- ☐ Controleer dit opnieuw na elke abonnementsupgrade
- ☐ Maak een lijst van goedgekeurde AI-tools voor je team
- ☐ Leg intern vast wie eindverantwoordelijk is voor AI-output
- ☐ Check of je AI-leveranciers een verwerkersovereenkomst hebben getekend
- ☐ Gebruik betaalde versies voor alle zakelijk AI-gebruik

Wil je meer weten over AI-security?

Security is één van de vijf thema's in onze blog The Dark Side of AI. Ontdek hoe AI in marketing en sales risico's introduceert, zoals datalekken door het delen van gevoelige informatie in AI-tools. We vertalen deze en andere onderwerpen, zoals desinformatie, deepfakes, bias, vendor lock-in en milieu-impact, naar concrete situaties uit de dagelijkse praktijk.

[Lees de blog: The Dark Side of AI](#)



AI security: 5 risico's die iedere B2B marketeer moet kennen

Vragen over AI security in jouw organisatie?

Wij helpen marketing- en salesteams om AI veilig en effectief te implementeren.

Mark van Horik

Strategic Marketing Consultant

Hulp nodig? Neem contact op



MG

MARKETING GUYS

Maanlander 39 ■ 3824 MN Amersfoort ■ +31(0)337370250

info@marketingguys.nl ■ www.marketingguys.nl