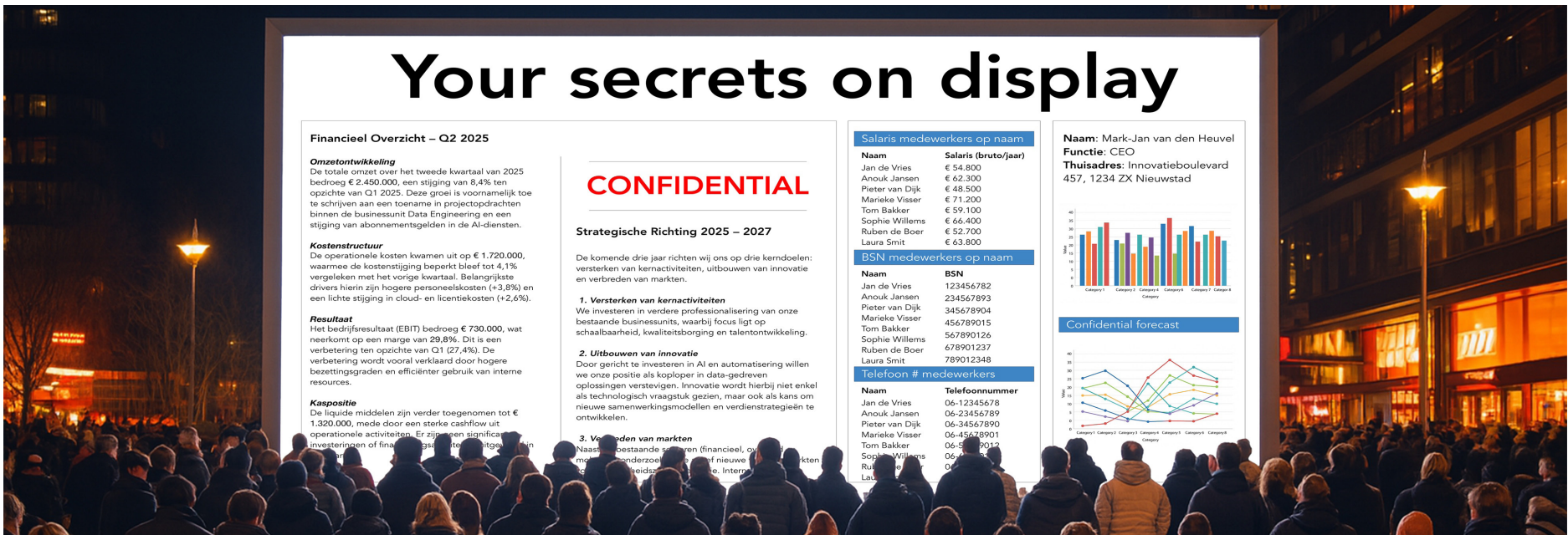




Voorkom dat AI je geheimen verradt – houd grip op je data

Organisaties werken volop met generatieve AI, maar staan zelden stil bij de vraag waar hun data wordt opgeslagen en wie er toegang toe heeft. Alleen als je weet waar je data is en welke regels gelden, houd je grip op het gebruik ervan en ligt niet alles zomaar op straat. Deze datasoevereiniteit is een cruciale randvoorwaarde voor veilige, betrouwbare en toekomstbestendige AI-toepassingen. Ook helpt het bedrijven om te voldoen aan privacyregels en andere wetgeving rondom datagebruik.



Francesca Brzowski,
AI strategy & engineering lead,
Puur Data

De adoptie van generatieve AI gaat razendsnel. Steeds meer medewerkers gebruiken tools als ChatGPT of Claude om sneller te schrijven, analyseren of presenteren. Maar al te vaak zonder oog voor wat er met de ingevoerde data gebeurt. “Organisaties realiseren zich vaak niet dat hun informatie letterlijk naar een andere plek wordt gestuurd, buiten hun invloedssfeer”, zegt Francesca Brzowski, AI strategy & engineering lead bij Puur Data, een bedrijf dat organisaties helpt om hun AI-toepassingen veilig, pragmatisch en datasoeverein in te richten.

Een recent voorbeeld onderstreept dat risico. Door een fout in de instellingen van ChatGPT werden gedeelde chats via Google vindbaar. Zo kwamen gevoelige gegevens zoals e-mailwisselingen, samenvattingen van vertrouwelijke vergaderingen en zelfs medische informatie onbedoeld openbaar op internet te staan. “Dat wil je als organisatie koste wat het kost voorkomen”, stelt managing director Marco van den Brandhof. “Zeker als het gaat om interne documenten, klantgegevens of financiële rapporten.”

Lokale opslag

Datasoevereiniteit betekent dat organisaties zelf bepalen waar hun data staat, wie er toegang toe heeft en onder welke wetgeving die valt. Brzowski: “Veel AI-modellen worden in de cloud gehost, vaak bij buitenlandse aanbieders. Dan gelden buitenlandse wetten, ook als jouw bedrijf in Nederland zit.”

Lokale opslag van data en AI-toepassingen helpt om controle te houden. “Dat betekent niet dat alles per se op je eigen server gehost moet worden”, nuanceert Van den Brandhof. “Maar je moet wel weten waar je data is en wie erbij kan. De data die je vorige week in een AI-prompt hebt getypt, kan nu op een server in een ander land staan, onder wetten die je nooit hebt gelezen.”



Houd AI lokaal en je data veilig

Veilige alternatieven

Steeds meer ontwikkelaars bieden downloadbare modellen aan die je offline kunt gebruiken. Deze modellen zijn vooral interessant voor organisaties die met gevoelige gegevens werken, zoals overheidsinstanties, zorginstellingen of financiële bedrijven. Ook kleinere bedrijven die meer controle willen over hun data kunnen hiervan profiteren. Organisaties kunnen deze modellen lokaal installeren en trainen, zodat hun data intern blijft. Van den Brandhof: “Wij bouwen ook

vaak hybride oplossingen: data en modellen draaien lokaal, maar AI kan via eenrichtingsverkeer wel externe bronnen raadplegen. Zo profiteer je van praktische AI-inzichten, zoals het automatisch samenvatten van documenten of het herkennen van trends in marktrapporten, zonder risico op datalekken.”

Dat is niet alleen veiliger, maar vaak ook efficiënter. “Met Search AI kan een zorginstelling in seconden patiëntendossiers doorzoeken, zonder gevoelige gegevens buiten de eigen omgeving te brengen”, vertelt Brzowski. In een hybride model kun je bovendien je interne gegevens vergelijken met externe gegevens en trends. Zo krijg je aanvullende marktgegevens zonder interne informatie prijs te geven.

Een kwestie van bewustwording

Toch staan veel organisaties nog onvoldoende stil bij datasoevereiniteit. Ze zien vooral de voordelen van AI, zoals tijdwinst en gemak. “AI wordt vaak omarmd vanwege de productiviteitswinst”, zegt Van den Brandhof. “Maar het gesprek over waar de ingevoerde data terecht komt, blijft vaak achterwege. Terwijl dat net zo belangrijk is voor de veiligheid van je organisatie.”

Wanneer mensen aan AI denken, denken ze vaak aan ChatGPT. Maar AI is veel krachtiger en risicovoller wanneer het is ingebouwd in de systemen waarop je je bedrijf runt. Het advies van Puur Data: begin klein en praktisch. Kijk eerst welke AI-tools je gebruikt. Denk daarbij niet alleen aan voor de hand liggende tools zoals ChatGPT, maar ook aan andere slimme software. Noteer welke gegevens je invoert in deze tools. Gaat het bijvoorbeeld om klantgegevens, financiële informatie of interne documenten? Breng ook in kaart wat er met die data gebeurt en waar het uiteindelijk terecht komt. Brzowski: “Zo krijg je inzicht in mogelijke risico’s. Daarna kun je beter beslissen of je je huidige tools veilig kunt blijven gebruiken, of dat je moet overstappen op een veiliger alternatief.”



Marco van den Brandhof,
Managing director, Puur Data

Grip op de toekomst

AI brengt risico’s met zich mee, maar wie weet waar zijn data staat en hoe die worden gebruikt, beheerst die risico’s. Zet datasoevereiniteit daarom vandaag nog op de agenda van je organisatie. Puur Data helpt daarbij van eerste analyse tot veilige implementatie. Wie grip houdt op zijn data, houdt grip op AI.

Factbox

Puur Data levert slimme en betrouwbare data- en AI-oplossingen aan overheden, zorginstellingen en bedrijven. Het bedrijf is specialist in Elastic-technologie en combineert sectorspecifieke kennis met een pragmatische aanpak. Hun expertise omvat onder meer semantisch zoeken in miljoenen documenten, machine learning op gevoelige datasets zonder dat deze de omgeving verlaten, natuurlijke interactie met interne kennisbanken, automatische herkenning van documenten en contracten, en de inzet van AI-agents die zelfstandig acties uitvoeren. Met ervaring in AI Search, vector databases en hybride architecturen helpt Puur Data organisaties om datasoevereiniteit te waarborgen en tegelijkertijd de mogelijkheden van AI optimaal te benutten.

