Vindex
POWERED BY FLORIJN

Digitale soevereiniteit en regie over Ai

Waarom het grootste Ai-risico voor het mkb niet in de techniek zit, maar in de vraag wie de regie heeft .

Whitepaper voor directie, CFO's en operationeel managers in het mkb

Whitepaper

Barentszplein 6B
1013 NJ Amsterdam

+31 (0) 20 6 254 254

https://vindex.nl/

In het kort

Ai is in het groot mkb geen experiment meer. Bijna de helft van de bedrijven met 50 tot 250 medewerkers gebruikt het al. [1] De vraag is dus niet of je Ai inzet, maar hoe je dit intern vormgeeft. Waar gaat je data naartoe, wat mag Ai doen, wordt jouw data gebruikt om het Ai model verder te trainen of wat gebeurt er als je Ai leverancier wegvalt?

Dat is digitale soevereiniteit: de ruimte om zelf keuzes te maken over technologie, data en leveranciers. Wie die regie niet bewust organiseert, geeft haar ongemerkt uit handen. Aan medewerkers met een gratis chatbot, aan leveranciers met hun eigen voorwaarden en aan buitenlandse wetgeving.

Dit whitepaper laat zien welke risico's je vandaag al loopt, wat de AVG en de AI Act concreet van je vragen en hoe je Ai zo inzet dat jij de regie houdt.

> ***Onze stelling: wie niet kiest, heeft al gekozen. In veel organisaties wordt het Ai-beleid vandaag geschreven door medewerkers met een gratis account.***

1 Je medewerkers gebruiken al Ai. Heb jij het overzicht?

Begin met drie vragen. Welke Ai-tools gebruiken je medewerkers vandaag? Welke klant-, personeels- of financiële gegevens gaan daarin? En op welke servers, onder welke voorwaarden, belandt die informatie?

Weinig directies kunnen dat precies beantwoorden. Wereldwijd gebruikt 75% van de kenniswerkers Ai op het werk, en 78% van hen neemt daarvoor eigen tools mee. [2] De Autoriteit Persoonsgegevens (AP) ontving meerdere datalekmeldingen omdat medewerkers persoonsgegevens in een Ai-chatbot hadden gezet: patiëntgegevens bij een huisartsenpraktijk, een bestand met klantadressen bij een telecombedrijf. [3] In 2025 kreeg de AP meer van zulke meldingen dan in 2024. [4]

Dat is geen verwijt aan medewerkers. Zij zoeken de snelste weg om hun werk goed te doen. Het is wel een signaal aan de directie: **als de organisatie geen veilig alternatief biedt, kiest de werkvloer er automatisch zelf een.**

2 Vijf risico's die je vandaag al loopt

Digitale soevereiniteit klinkt abstract. De risico's zijn dat niet.

1. **Datalekken via publieke Ai-tools.** Wat een medewerker in een gratis chatbot plakt, staat op de servers van de aanbieder. Zitten daar persoonsgegevens in, dan is het al snel een datalek dat je binnen 72 uur bij de AP moet melden. [3], [5]
2. **Toegang door buitenlandse overheden.** Een aanbieder onder Amerikaanse rechtsmacht kan onder de US CLOUD Act worden verplicht gegevens te verstrekken, ongeacht waar de server staat. [6] Microsoft France kon onder ede niet garanderen dat dit nooit gebeurt. [7]
3. **Afhankelijkheid en lock-in.** Een leverancier verandert prijzen, voorwaarden of modellen, of de dienst valt uit. Hoe lang kan je organisatie dan door? Zelfs van de zeer grote Nederlandse organisaties in het onderzoek van Capgemini heeft slechts 16% volledig zicht op de eigen digitale leverancierssketen. [8]
4. **Fouten die niemand ziet.** Een taalmodel kan zich vergissen en geeft op dezelfde vraag niet altijd hetzelfde antwoord. Een agent met te veel rechten voert die fout direct door in je systemen. Ook aanvallers richten zich op Ai: bij ruim een op de vijf onderzochte organisaties was een aanval gericht op Ai-modellen of

-applicaties, meestal via zwakke plekken eromheen, zoals API's en plug-ins en verkeerd ingerichte cloudomgevingen (27%). [9]

5. **Boetes en bestuurlijke verantwoordelijkheid.** De AVG kent boetes tot €20 miljoen of 4% van de wereldwijde jaaromzet. [5] De AI Act gaat tot €35 miljoen of 7% voor verboden toepassingen; voor mkb-bedrijven geldt het laagste van die twee bedragen. [10] En onder de Cyberbeveiligingswet is het bestuur zelf verantwoordelijk voor het goedkeuren van en toezicht houden op de beveiliging. [11]

3 Wat de AVG en de AI Act concreet van je vragen

Je hoeft geen jurist te zijn om de hoofdlijnen te kennen. Voor de meeste mkb-organisaties komt het neer op dit overzicht.

Regel	Geldt vanaf	Wat het voor jou betekent
AVG	25 mei 2018	Gebruik je persoonsgegevens in Ai, dan verwerk je ze. Je hebt een grondslag en een duidelijk doel nodig, een verwerkersovereenkomst met elke Ai-leverancier en bij gevoelige of grootschalige verwerking een DPIA. Gegevens gaan alleen met passende waarborgen buiten de EU. Een datalek meld je binnen 72 uur.
AI Act: Ai-geletterdheid	2 februari 2025	Medewerkers die met Ai werken, moeten weten wat het kan, wat het niet kan en welke risico's eraan kleven. Denk aan training en heldere werkafspraken over welke gegevens wel en niet in Ai mogen.
AI Act: transparantie	2 augustus 2026	Publiceer je Ai-gegenereerde beelden, audio of video die echt lijken (deepfakes), dan meld je dat. Klanten moeten weten dat ze met Ai communiceren; controleer of je chatbotleverancier daarvoor zorgt.
AI Act: hoog risico	2 december 2027	Ai bij werving en selectie, beoordeling van medewerkers of kredietwaardigheid valt onder strengere regels. Als gebruiker regel je menselijk toezicht, bewaar je logs en informeer je medewerkers vooraf.
Cyberbeveiligingswet (NIS2)	15 augustus 2026	Geldt voor organisaties in aangewezen sectoren, doorgaans vanaf 50 medewerkers of met meer dan €10 miljoen omzet. Het bestuur keurt de maatregelen goed en houdt toezicht. Check eerst of je eronder valt.

Bronnen bij dit overzicht: [5], [8].

Twee nuances die vaak worden gemist. Ten eerste ben je als mkb'er onder de AI Act meestal 'gebruiksverantwoordelijke', niet 'aanbieder'. Dat beperkt je verplichtingen, maar je blijft verantwoordelijk voor hoe je Ai inzet. Ten tweede vervangt Nederlandse of Europese hosting geen van deze verplichtingen. Het maakt het wel een stuk eenvoudiger om eraan te voldoen, omdat je weet waar de data staat en wie erbij kan.

> ***Onze stelling: compliance is de ondergrens, niet het doel. Wie Ai alleen inricht om de toezichthouder tevreden te houden, mist waar het werkelijk om gaat: grip op de eigen bedrijfsvoering.***

4 Regie toets je met drie vragen

Een organisatie heeft meer nodig dan de zekerheid dat haar data in Nederland of Europa staat. Of je echt regie hebt, toets je met drie vragen.

Kunnen we zien wat er gebeurt?

Welke gegevens gebruikt een toepassing? Wie heeft toegang? Welke acties voert zij uit en waar worden uitzonderingen vastgelegd? Inzicht vraagt om actuele informatie over de inrichting én de dagelijkse werking. Een bronverwijzing helpt een antwoord te controleren, maar bewijst niet dat het antwoord klopt.

Zijn verantwoordelijkheden en bevoegdheden duidelijk vastgelegd?

Wie bepaalt de taak, de toegang en de handelingsruimte van een toepassing? Wie keurt wijzigingen goed? Wie kan ingrijpen of de toepassing stilzetten? Leg deze bevoegdheden vast en controleer of de technische inrichting ermee overeenkomt.

Kunnen we verder als iets wegvalt?

Zijn data bruikbaar te exporteren? Kunnen koppelingen en configuraties worden overgedragen? Kan het werk tijdelijk handmatig door? Een alternatief telt pas als het uitvoerbaar is. Test daarom de belangrijkste uitwijk- en herstelafspraken.

Begin bij de processen die niet mogen uitvallen. Breng per proces in kaart welke systemen, gegevens, leveranciers en mensen nodig zijn. Dan zie je waar digitale afhankelijkheid echt pijn doet.

5 Waar je Ai draait, is een strategische keuze

De locatie van data is belangrijk, maar niet genoeg. Het criterium is niet waar de server staat, maar wie de aanbieder is en onder welke rechtsmacht die valt. De CLOUD Act geeft geen onbeperkte toegang: er is een rechtsgeldig verzoek voor nodig. [6] Maar als klant kun je dat verzoek niet tegenhouden en je hoort er mogelijk niet van.

In de Franse Senaat werd de juridisch directeur van Microsoft France op 10 juni 2025 gevraagd of hij kon garanderen dat gegevens van Franse burgers nooit zonder akkoord van de Franse autoriteiten aan de VS worden overgedragen. Zijn antwoord: “Nee, dat kan ik niet garanderen, maar nogmaals, het is nog nooit gebeurd.” [7] Dat is een eerlijk antwoord. En het geeft precies aan waar het probleem zit.

Een Nederlandse private cloud met lokaal draaiende open modellen haalt die onzekerheid uit je kernprocessen. Je data verlaat de omgeving niet, wordt niet gebruikt om modellen van derden te trainen en valt onder Nederlands en Europees recht. Kijk wel naar de hele keten: hosting, beheer, back-ups, logging, externe koppelingen en subverwerkers. En open modellen maken overstappen makkelijker, maar alleen als ook je data, koppelingen en configuraties overdraagbaar zijn.

> ***Onze stelling: soevereiniteit is geen anti-Amerikaans sentiment. Het is goed ondernemerschap. Bouw je kernprocessen niet op juridische onzekerheden.***

6 Ai krijgt een taak en duidelijke grenzen

Ai kan documenten lezen, gegevens combineren en vervolgacties voorbereiden. Hoe meer zelfstandigheid, hoe explicieter de grenzen moeten zijn. Gebruik vaste regels voor controles die eenduidig moeten zijn, zoals bedragen vergelijken of verplichte velden controleren. Zet Ai in waar interpretatie nodig is, zoals informatie herkennen in een e-mail of document. En test beide samen in het werkelijke proces.

Voorbeeld: een agent voor inkomende facturen

Een factuur komt per e-mail binnen. De agent herkent het document, haalt de relevante gegevens eruit en vergelijkt die met de order- en leveranciersgegevens. Hij bereidt een boeking voor en legt vast welke controles zijn uitgevoerd.

De taak is afgebakend. De agent heeft toegang tot de factuurmailbox en de benodigde financiële gegevens, niet tot personeelsdossiers. Bankgegevens wijzigen en betalingen uitvoeren vallen buiten zijn bevoegdheid.

De organisatie bepaalt vooraf wat automatisch mag, bijvoorbeeld het registreren van een factuur die aan alle controles voldoet. Ontbreekt informatie, wijkt het rekeningnummer af of is de herkenning onzeker, dan gaat het dossier naar een medewerker. Die ziet de oorspronkelijke factuur, de uitgevoerde controles en de reden waarom beoordeling nodig is.

De proceseigenaar bepaalt de grenzen, de techniek dwingt ze af, de medewerker behandelt de uitzonderingen. Zo blijft er altijd een 'human in the loop', zonder dat elke routinehandeling op een extra akkoord hoeft te wachten.

Controle die in het dagelijks werk past

Beleid beschrijft wat mag. Audits toetsen of de inrichting klopt. Dagelijkse monitoring laat zien of de toepassing in de praktijk goed blijft werken. Je hebt alle drie nodig. Breng daarom niet alleen hoeveel werk de agent verwerkt, maar ook onjuiste uitkomsten, gemiste afwijkingen, onnodige meldingen en het herstelwerk voor medewerkers in kaart. En beoordeel wijzigingen aan modellen, bronnen en koppelingen voordat ze live gaan.

> ***Onze stelling: de efficiëntste Ai-toepassingen zijn saai. Ze doen routinematige handelingen, elke dag hetzelfde en besparen daarmee vooral tijd.***

7 Begin klein, maar begin

Het bestuur bepaalt hoeveel afhankelijkheid en risico de organisatie accepteert. IT vertaalt dat naar de technische inrichting. De proceseigenaar bepaalt wat Ai moet doen en wanneer een medewerker nodig is. Zo krijgt regie een eigenaar en wordt zij onderdeel van de bedrijfsvoering, in plaats van een IT-project.

Vijf vragen voor je volgende directieoverleg

- Welke Ai-tools gebruiken onze medewerkers nu en welke gegevens gaan erin?
- Welke processen mogen niet uitvallen en van welke leveranciers zijn ze afhankelijk?
- Welke gegevens en acties zijn per Ai-toepassing toegestaan en wie keurt wijzigingen goed?
- Wie controleert de uitkomsten, en wie behandelt de uitzonderingen?
- Kunnen we overstappen of doorwerken als deze leverancier wegvalt?

Kies één proces. Leg de uitgangssituatie vast en bepaal wat beter moet: minder handwerk, kortere doorlooptijd of minder herstelwerk. Spreek tegelijk af welke fouten onacceptabel zijn en wanneer een medewerker moet beoordelen. Test met echte gebruikers en representatieve situaties, inclusief uitzonderingen. Niets doen en wachten tot alles is uitgezocht, is ook een keuze, maar meestal de duurste.

De Vindex-gedachte: jouw data, jouw Ai

Wij geloven dat Ai pas echt waarde toevoegt als je het kunt vertrouwen. Niet blind, maar omdat je kunt zien wat het doet. Daarom bouwen we Ai volgens vier principes.

- **In Nederland, onder Europees recht.** Onze Ai-agents draaien in een Nederlandse private cloud en met open modellen. Je data verlaat die omgeving niet en wordt niet gebruikt om modellen van derden te trainen.
- **Eén Ai-laag in plaats van losse tools.** De agents werken op je bestaande systemen, zoals ERP, CRM en SharePoint, met centraal geregelde toegang, logging en beheer. Geen wildgroei aan losse tools, agents en abonnementen.
- **Uitlegbaar en begrensd.** Elke stap is herleidbaar tot de gebruikte bron. De agent doet alleen wat is afgesproken; uitzonderingen gaan naar een medewerker.
- **Klein beginnen, aantoonbaar resultaat.** We starten met één afgebakend proces, leggen de uitgangssituatie vast en meten KPI's voordat we uitbreiden.

Concreet onderzoeken we samen de benodigde gegevens, koppelingen, toegangsrechten en risico's. We bepalen de taak van de agent en wanneer menselijk akkoord nodig is, testen met echte gebruikers en richten beheer en monitoring in.

Ai die voor je werkt. Jij bepaalt hoe.

In een vrijblijvende kennismaking bespreken we waar jouw organisatie tijd verliest en welke regie nodig is om Ai daar betrouwbaar te laten meewerken.

Plan een kennismakingsgesprek via vindex.nl/contact

Vindex.nl | info@vindex.nl | +31 (0)20 6 254 254

Bronnen en verantwoording

Bronnen gecontroleerd op 8 oktober 2026. Onderzoeksresultaten gelden voor de onderzochte doelgroep en vormen geen garantie voor de uitkomsten van een specifieke Ai-toepassing. Dit whitepaper geeft een algemeen beeld en is geen juridisch advies; laat je bij twijfel over de toepasselijkheid van wetgeving adviseren.

[1] CBS. Bedrijven gebruiken AI vaakst voor marketing of verkoop. 12 december 2025. Voorlopige cijfers over 2025; aangehaald: bedrijven met 50 tot 250 werkzame personen.

Bekijk de bron

[2] Microsoft en LinkedIn. 2024 Work Trend Index: AI at work is here. Now comes the hard part. 8 mei 2024. Wereldwijd onderzoek onder 31.000 werkenden in 31 landen; geen specifiek Nederlandse cijfers.

Bekijk de bron

[3] Autoriteit Persoonsgegevens, via Dutch IT Channel. AP: gebruik AI-chatbot kan leiden tot datalekken.

7 augustus 2024. Waarschuwing van de AP naar aanleiding van datalekmeldingen.

Bekijk de bron

[4] Accountant.nl. AP slaat alarm over datalekken door AI. 30 december 2025. Op basis van berichtgeving in het FD; de AP ontving in 2024 en 2025 tientallen meldingen.

Bekijk de bron

[5] Algemene verordening gegevensbescherming (AVG). Verordening (EU) 2016/679, onder meer art. 33 (melden datalek binnen 72 uur) en art. 83 (boetes).

Bekijk de bron

[6] US Department of Justice. Justice Department Announces Publication of White Paper on the CLOUD Act. 10 april 2019; pagina bijgewerkt 5 februari 2025. Primaire toelichting op rechtsmacht en gegevens onder zeggenschap van aanbieders.

Bekijk de bron

[7] Sénat. Commission d'enquête sur la commande publique. Verhoor van Anton Carniaux en Pierre Lagarde van Microsoft France, 10 juni 2025. Citaat vertaald uit het Franse verslag: « Non, je ne peux pas le garantir, mais, encore une fois, cela ne s'est encore jamais produit. »

Bekijk de bron

[8] AI Geletterdheid. AI Act-verplichtingen voor organisaties. Overzicht van verplichtingen per risicocategorie, AI-geletterdheid en verantwoordelijkheden binnen organisaties. Bijgewerkt op 28 september 2026.

Bekijk de bron