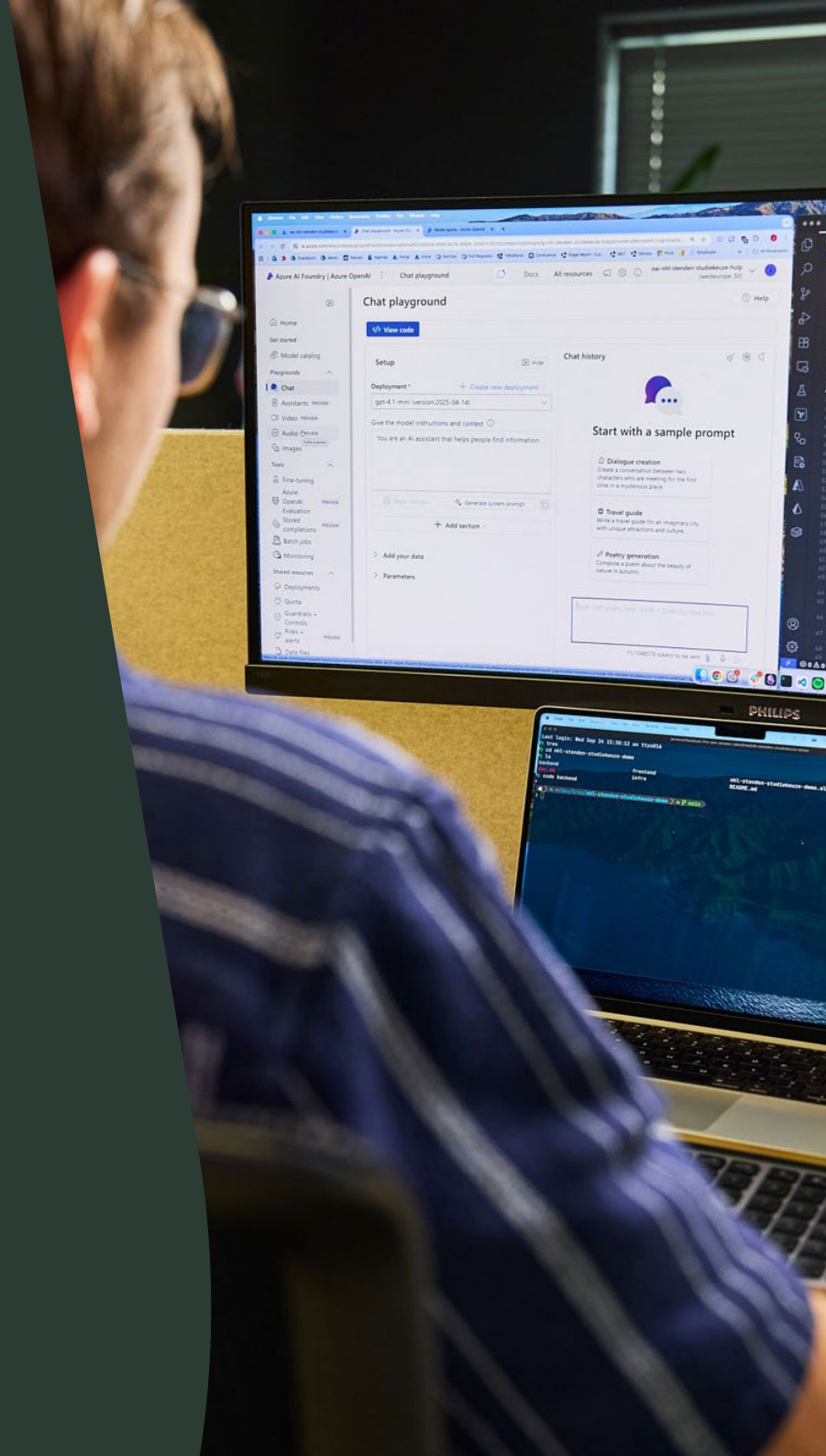
TRES

AI zonder risico



Whitepaper

Hoe organiseer je AI veilig, beheersbaar en toekomstbestendig?

AI biedt enorme kansen. Processen worden efficiënter. Kennis wordt direct toegankelijk. Professionals winnen tijd. Organisaties worden wendbaarder.

Maar zonder grip wordt AI een risico.

In veel organisaties gebruiken medewerkers al publieke AI-tools. Vaak zonder duidelijke richtlijnen. Gevoelige informatie wordt gekopieerd in chatvensters. Antwoorden worden direct verwerkt in documenten. De efficiëntie stijgt, maar controle ontbreekt.

De vraag voor organisaties is niet of zij AI inzetten, maar hoe zij dit verantwoord, beheersbaar en toekomstbestendig organiseren.

In deze whitepaper lees je hoe je AI-veiligheid structureel organiseert. Van governance en eigenaarschap tot een afgeschermde Private AI-omgeving die innovatie mogelijk maakt zonder concessies aan controle.

1. De realiteit: AI wordt al gebruikt

AI is geen toekomstmuziek. Het is dagelijkse praktijk.

Medewerkers gebruiken tools om rapportages te versnellen. Juristen analyseren documenten. Zorgprofessionals structureren dossiers. Accountants laten teksten herschrijven.

Vaak gebeurt dit buiten IT om.

Dit zogenaamde ‘shadow AI’-gebruik brengt risico’s met zich mee:

» Gevoelige data wordt gedeeld met externe modellen
» Er is geen zicht op wat wordt ingevoerd
» Compliance-eisen zijn niet geborgd
» Data kan onderdeel worden van externe trainingssets

Voor organisaties die werken met vertrouwelijke informatie (zoals advocaten, zorginstellingen of accountants) is dit geen theoretisch risico. Het raakt direct aan privacy, reputatie en aansprakelijkheid.

AI versnelt processen, maar zonder structuur versnelt het ook risico’s.

2. Wat betekent ‘AI zonder risico’ eigenlijk?

Veel organisaties denken bij AI-veiligheid alleen aan opslag. Waar staat de data?

Maar veiligheid is breder. AI-veiligheid bestaat uit vijf lagen.

1. **Data-eigenaarschap**
   Blijft jouw data binnen je eigen infrastructuur? Of wordt deze verwerkt in externe omgevingen?
2. **Modelisolatie**
   Wordt jouw input gebruikt om publieke modellen verder te trainen? Of draait het model exclusief binnen jouw omgeving?
3. **Toegangsbeheer**
   Wie mag wat vragen? Wie heeft toegang tot welke kennisbronnen?
4. **Governance**
   Wie is verantwoordelijk voor AI-beleid? Wie bewaakt compliance en kwaliteit?
5. **Monitoring en doorontwikkeling**
   Hoe controleer je gebruik, risico’s en prestaties? En hoe stuur je bij?

AI zonder risico betekent niet dat er geen risico’s zijn. Het betekent dat je ze beheerst.

3. De drie fases van AI-volwassenheid

Organisaties doorlopen meestal drie fases.

Fase 1 – Experimenteren

Medewerkers gebruiken publieke tools. Er is geen beleid. Geen centrale controle.

AI levert snelheid op, maar geen strategische grip.

Fase 2 – Gereguleerd gebruik

Er komen richtlijnen. Gebruik wordt beperkt. IT krijgt zicht op toepassingen.

De risico's worden kleiner, maar eigenaarschap ontbreekt nog.

Fase 3 – Private AI

AI draait binnen een eigen, afgeschermde omgeving. Data blijft binnen de organisatie. Gebruik is geïntegreerd in processen. Hier ontstaat gecontroleerde innovatie. Dit is het punt waarop AI niet alleen efficiëntie oplevert, maar bijdraagt aan digitale ambitie.

4. Hoe borg je AI-veiligheid structureel?

Veiligheid organiseer je op vier niveaus.

4.1 Technische inrichting

Een veilige AI-omgeving begint bij infrastructuur.

- Een eigen Microsoft Azure omgeving, gehost in West-Europa.
- Een afgeschermd GPT-model binnen jouw omgeving.
- Geen datadeling met externe partijen.
- Open source componenten voor flexibiliteit.

Hiermee behoud je volledige controle over data, infrastructuur en beveiligingsinstellingen. Solide technologie is de basis voor vertrouwen en continuïteit.

4.2 Procesinrichting

Techniek zonder proces leidt alsnog tot risico's. Richt daarom het volgende in:

- AI-gebruiksbeleid
- Autorisatiestructuur
- Logging en monitoring
- Compliance-checks

AI wordt daarmee onderdeel van je bestaande governance-structuur.

4.3 Mensen en adoptie

AI is meer dan alleen een IT-project, het raakt de dagelijkse praktijk.

Professionals moeten weten:

» Wat ze wel en niet mogen delen
» Hoe ze AI verantwoord inzetten
» Hoe ze output controleren

Training en bewustwording zijn erg belangrijk. Wanneer medewerkers begrijpen hoe AI veilig werkt, groeit vertrouwen. En daarmee adoptie.

4.4 Doorontwikkeling

Digitale ambitie is nooit af. Nieuwe use cases ontstaan. Wetgeving verandert. Technologie ontwikkelt zich. Organiseer daarom periodieke evaluatie:

» Welke processen versnellen we nog meer?
» Waar zitten nieuwe risico's?
» Hoe optimaliseren we kwaliteit?

AI wordt op deze manier een structurele innovatie-laag binnen je organisatie.

5. Praktijkvoorbeeld: veilige AI in de juridische praktijk

Een vastgoedadvocatenkantoor werkte dagelijks met omvangrijke en vertrouwelijke dossiers. Denk aan huurgeschillen, burenconflicten en incassotrajecten. Elk dossier bestond uit tientallen documenten, e-mails en processtukken.

Het analyseren en structureren van deze informatie kostte gemiddeld 2 tot 3 uur per zaak. Tegelijk mocht geen enkele cliëntinformatie buiten de organisatie terechtkomen. Publieke AI-tools waren daarom geen optie.

De organisatie wilde versnellen, zonder concessies te doen aan vertrouwelijkheid.

Door AI binnen een volledig afgeschermde Private AI-omgeving te implementeren:
» Werden complete dossiers automatisch omgezet in overzichtelijke tijdlijnen
» Werden eerste versies van juridische documenten gegenereerd op basis van interne kennis
» Kon uitsluitend worden gewerkt met data binnen de eigen infrastructuur
» Werd per rol bepaald welke informatie zichtbaar was

Het resultaat na zes maanden:
» 40% tijdsbesparing op dossieranalyse
» Kortere doorlooptijden richting cliënten
» Minder handmatige fouten in standaarddocumenten
» Volledig behoud van data-eigenaarschap

Een van de advocaten gaf aan:
"Het voelt alsof we een extra juridisch medewerker hebben, zonder dat we ook maar één risico lopen met cliëntinformatie."

6. Stappenplan: zo maak je AI veilig binnen jouw organisatie

Wil je AI veilig organiseren? Begin dan zo:

1. Breng huidig AI-gebruik in kaart.
2. Identificeer risicogevoelige data.
3. Bepaal eigenaarschap en verantwoordelijkheden.
4. Kies een infrastructuurmodel dat data-eigenaarschap garandeert.
5. Richt governance en autorisaties in.
6. Start gecontroleerd met een afgebakende use case die je kunt valideren op effectiviteit en bruikbaarheid.
7. Evalueer en schaal op.

Zo voorkom je dat AI een ongecontroleerd experiment blijft en maak je het onderdeel van je digitale strategie.

7. AI als fundament voor gecontroleerde innovatie

Organisaties die AI goed organiseren, versnellen innovatie. Niet ondanks veiligheid, maar dankzij veiligheid.

Wanneer data binnen de organisatie blijft en governance helder is ingericht, ontstaat ruimte om te experimenteren. Dan durven teams nieuwe toepassingen te ontwikkelen.

AI wordt dan een fundament onder verdere digitale groei. En precies daar wordt digitale ambitie waargemaakt.

Conclusie

AI zonder risico bestaat niet. Maar AI zonder controle is geen optie.

Door te kiezen voor een Private AI-omgeving met duidelijke governance en eigenaarschap, maak je van AI een strategische kracht in plaats van een compliance-uitdaging.

Zo benut je de voordelen van generatieve AI. Zonder concessies te doen aan privacy, betrouwbaarheid of controle.

AI binnen jouw organisatie: hoe is dit geregeld?

AI wordt waarschijnlijk al gebruikt binnen jouw organisatie. De vraag is: heb je het onder controle?

Wil je weten hoe kwetsbaar jouw organisatie vandaag is voor ongecontroleerd AI-gebruik? In één strategische sessie brengen we in kaart:

» Hoe AI nu binnen jouw organisatie wordt gebruikt.
» Waar de grootste privacy- en compliance-risico's zitten.
» In welke AI-volwassenheidsfase je je bevindt.
» Welke concrete vervolgstappen nodig zijn om veiligheid te borgen.

Je gaat naar huis met een helder risicoprofiel en een concreet stappenplan. Zo krijg je direct inzicht in hoe je AI veilig, beheersbaar en toekomstbestendig organiseert.

Meer weten?

Neem contact met ons op.

Bouke Weening

Commercieel manager

boukeweening@tres.nl

+31 (6) 55 22 33 53

TRES Maakt digitale ambitie waar.