AI-geletterdheid als complianceplicht

Voorkom boetes, bias en black-box risico's in bestaande governance

Inhoud

01	**De blinde vlek in AI-governance**	3
02	**AI-geletterdheid als wettelijke verplichting**	4
03	**Wat de EU AI Act voor u betekent**	5
	Implementatietijdlijn van de AI Act	6
	Aansluiten bij bestaande compliance	6
04	**De hoge prijs van onwetendheid**	7
05	**AI-governance in de praktijk brengen**	8
	Checklist voor AI-compliance binnen uw bestaande frameworks	9
06	**Smart learning als brug naar compliance**	10
	Serious Training in de praktijk	10
	Maatwerk expertise voor elke rol binnen uw organisatie	11
	Risico-inventarisatie als solide fundament	11
07	**Voorsprong door slimme integratie**	12
08	**Referenties**	13

01

De blinde vlek in AI-governance

70% van de Nederlandse organisaties implementeert AI-systemen zonder adequate governance of risicobeheer, zo blijkt uit het recente "AI & Algorithmic Risks Report" (Autoriteit Persoonsgegevens, 2024). Als security- of complianceprofessional sta je waarschijnlijk al voor de uitdaging om deze nieuwe technologieën veilig te integreren binnen uw organisatie - misschien zelfs zonder dat je er expliciet van op de hoogte bent.

De vraag is niet óf jouw organisatie AI gebruikt, maar waar het precies gebeurt en of u de bijbehorende risico's onder controle heeft. Met de inwerkingtreding van de AI-verordening sinds februari 2025 zijn organisaties nu wettelijk verplicht werk te maken van AI-geletterdheid - een verplichting die direct raakt aan jouw bestaande verantwoordelijkheden binnen ISO 27001:2022, NIS2 en AVG-compliance.

Je staat voor een groeiende uitdaging: binnen uw organisatie worden steeds meer AI-systemen geïmplementeerd, maar er is onvoldoende zicht op welke algoritmen precies worden gebruikt en waar. Deze blinde vlek creëert ernstige compliance-risico's die direct raken aan jouw verantwoordelijkheden.

Dit whitepaper biedt je een concrete routekaart om AI-geletterdheid te verankeren in jouw bestaande governance-raamwerk. De belangrijkste boodschap:

AI-compliance is geen losstaand domein dat compleet nieuwe expertise vereist, maar een risico dat je kunt beheersen met jouw vertrouwde werkwijze in risicomanagement.

02 AI-geletterdheid als wettelijke verplichting

Volgens de Digitale Overheid (2025) is AI-geletterdheid 'een verzamelnaam voor kennis en kunde op het vlak van Artificiële Intelligentie. Denk bijvoorbeeld aan dat men weet hoe deze technologie (op basaal niveau) werkt, waar de kansen liggen en welke risico's er aan verbonden zijn. Hierbij gaat het dus niet alleen om technische kennis, maar ook om sociale, ethische en praktische aspecten'. Deze definitie omvat zowel organisaties die AI-systemen implementeren en ontwikkelen als medewerkers die dagelijks gebruikmaken van AI-tools zoals ChatGPT, Copilot, generatieve zoekmachines of andere AI-gestuurde applicaties. Voor beide groepen geldt: zonder voldoende kennis van de mogelijkheden én beperkingen ontstaan risico's.

Als aanbieder of gebruiksverantwoordelijke van AI-systemen wordt in artikel 4 van de AI-verordening expliciet beschreven dat organisaties een toereikend niveau van AI-geletterdheid moeten waarborgen. **Deze verplichting is sinds februari 2025 van kracht**, wat het tot een actueel en urgent vraagstuk maakt voor security- en compliance-professionals.

De feiten spreken voor zich: diverse bronnen zoals Lumenova, IAPP en Frontiers in Human Dynamics wijzen erop dat de grootste risico's voor niet-naleving van AI-regelgeving voortkomen uit een gebrek aan AI-geletterdheid binnen organisaties, gevolgd door onvoldoende governance-structuren en een gebrek aan transparantie van AI-systemen.

Dit toont aan dat naleving van de EU AI Act niet enkel een technisch vraagstuk is, maar vooral een kwestie van investering in kennis bij medewerkers op alle niveaus, duidelijke governance-structuren met heldere verantwoordelijkheden, en uitlegbare AI-systemen die transparant zijn in hun werking.

03 Wat de EU AI Act voor u betekent

"De AI Act is de eerste alomvattende wettelijke regelgeving voor AI wereldwijd", stelt de Europese Commissie (2024). Wat deze wetgeving onderscheidt, is de risicogebaseerde benadering die naadloos aansluit bij bestaande security-frameworks zoals ISO 27001 – de taal die je al spreekt.

De vier risiconiveaus van de AI Act die je moet kennen:

1. **Verboden AI-praktijken (onaanvaardbaar risico):** Hieronder vallen schadelijke manipulatie en misleiding, exploitatie van kwetsbaarheden, ongerechtvaardigde sociale scoring en biometrische identificatie in de openbare ruimte (met strikte uitzonderingen).

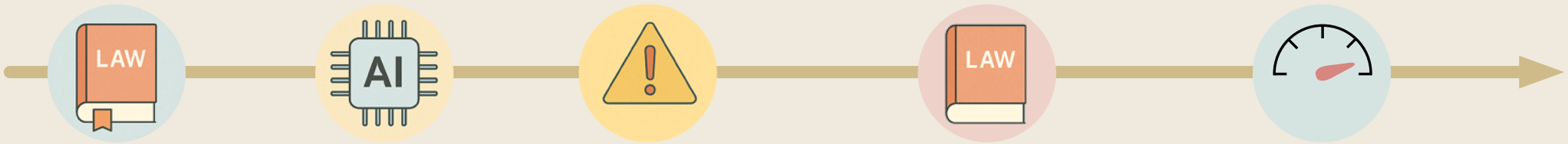
2. **Hoog-risico AI-systemen:** Deze zijn toegestaan onder strikte voorwaarden. Ze vereisen adequate risicobeoordelingen, uitgebreide logging van activiteiten, gedetailleerde documentatie en passende menselijke controle gedurende het hele proces.*

3. **Beperkt risico (transparantieverplichting):** In deze categorie moeten deepfakes herkenbaar zijn als manipulatie, gebruikers van chatbots moeten geïnformeerd worden dat ze met AI communiceren, en generatieve AI moet duidelijk aangeven dat content niet door mensen is gecreëerd.

4. **Minimaal of laag risico:** Voor de meeste AI-toepassingen gelden geen wettelijke verplichtingen.

** Komt dit je bekend voor? Dat is geen toeval – deze eisen sluiten direct aan bij je bestaande ISO 27001 en NIS2 implementaties.*

Implementatietijdlijn van de AI Act



Augustus 2024:
De AI-verordening is in werking getreden

Februari 2025:
Een half jaar na inwerkingtreding zijn de eerste verplichtingen van kracht geworden

Augustus 2025:
Eén jaar na inwerkingtreding worden de meeste verplichtingen van kracht

Augustus 2026:
Twee jaar na inwerkingtreding gaat de volledige AI-verordening gelden

Augustus 2030:
Alle AI-systemen bij overheidsorganisaties die vóór inwerkingtreding op de markt zijn gebracht moeten uiterlijk 6 jaar na inwerkingtreding van de verordening aan de eisen voor hoog risico AI-systemen voldoen

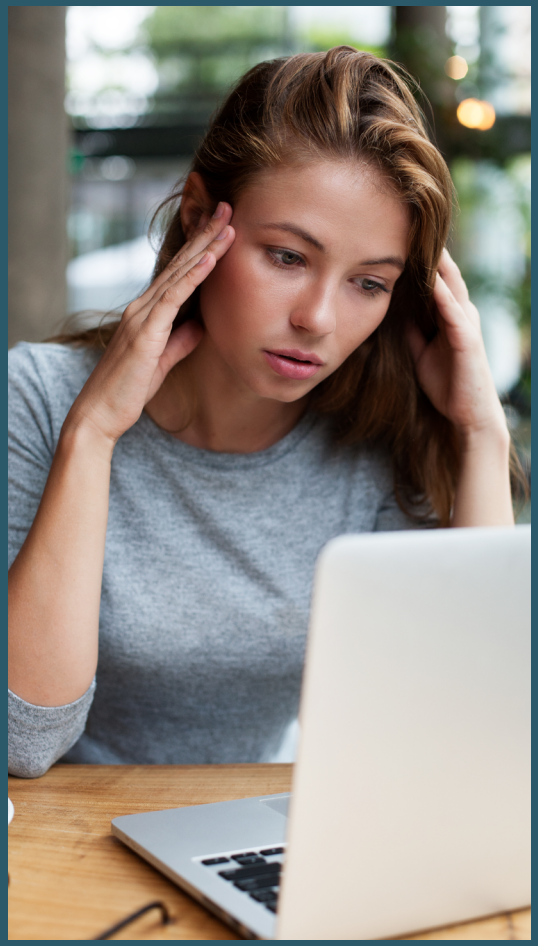
Aansluiten bij bestaande compliance
Voor jou als security- of compliance-professional is het essentieel om te begrijpen hoe de AI Act verweven is met regelgeving waar je al verantwoordelijk voor bent.

De NIS2-richtlijn raakt direct aan AI-systemen. Deze vereist passende risicobeheermaatregelen voor alle netwerk- en informatiesystemen in uw organisatie, waaronder AI-toepassingen. Onder NIS2 moet je incidenten binnen 24 uur melden en een gestructureerde aanpak hanteren voor incidentbehandeling, bedrijfscontinuïteit en de beveiliging van je toeleveringsketen. Deze eisen sluiten naadloos aan bij wat nodig is voor veilige AI-implementatie.

Ook de AVG blijft fundamenteel voor AI-systemen die persoonsgegevens verwerken. De principes van rechtmatige, eerlijke en transparante verwerking gelden onverminderd, net als de eisen rondom doelbinding en dataminimalisatie. Jouw organisatie moet blijven voldoen aan de normen voor integriteit, vertrouwelijkheid en verantwoordingsplicht. Voor AI-systemen betekent dit dat u aantoonbaar moet maken dat je modellen en gegevensverwerking in lijn zijn met deze principes – een uitdaging gezien de complexiteit van AI-technologieën.

De verwevenheid van deze regelgeving toont aan dat AI-governance geen volledig nieuw domein is, maar een logische uitbreiding van je bestaande compliance-kader.

04



De hoge prijs van onwetendheid

De EU AI Act introduceert strenge sancties voor organisaties die niet voldoen aan de nieuwe regelgeving. Deze sancties kunnen oplopen tot €35 miljoen of 7% van de wereldwijde jaaromzet bij ernstige overtredingen. Maar de werkelijke gevolgen reiken veel verder dan alleen financiële boetes.

Stel je de volgende situatie voor: jouw organisatie heeft een geavanceerd AI-systeem geïmplementeerd voor klantensegmentatie. Het systeem draait, classificeert klanten en beïnvloedt bedrijfsbeslissingen. Maar niemand binnen je organisatie begrijpt volledig hoe het werkt, welke data het precies gebruikt en welke criteria doorslaggevend zijn in de besluitvorming. Wat begint als een ogenschijnlijk onschuldige kenniskloof, kan uitgroeien tot een waterval van problemen.

Dit risico is niet beperkt tot complexe AI-implementaties. Ook alledaagse handelingen van medewerkers met generatieve AI-tools vormen een reëel gevaar. Zoals bijvoorbeeld, een medewerker die vertrouwelijke bedrijfsinformatie deelt met een publieke chatbot zonder zich bewust te zijn van de privacyrisico's. Of een marketingprofessional die AI-gegenereerde content publiceert zonder controle op feitelijke juistheid. Of wanneer een besluitvormer rapportages baseert op AI-analyses zonder de onderliggende beperkingen te begrijpen. Al deze scenario's kunnen leiden tot dezelfde compliance- en reputatierisico's.

De compliance-risico's zijn evident in het licht van de nieuwe AI-wetgeving. Naast potentiële boetes ontstaat er reputatieschade wanneer incidenten met jouw AI-systeem naar buiten komen, wat leidt tot verlies van vertrouwen bij klanten en partners. Zonder gedegen begrip van de technologie leidt implementatie ook tot suboptimaal gebruik – je haalt simpelweg niet het maximale uit uw investering. Ethische risico's liggen op de loer wanneer je AI-systeem onbedoeld discrimineert of vooroordelen bevat die je niet hebt opgemerkt. En wellicht het meest onderschat: je mist kansen omdat niemand binnen de organisatie de volledige potentie van de technologie begrijpt.

Deze risico's zijn geen theoretische dreigingen. Ze manifesteren zich dagelijks in organisaties die AI implementeren zonder voldoende kennis en governance. Dit is precies waarom AI-geletterdheid geen vrijblijvende keuze meer is. Het is een noodzakelijke competentie geworden binnen elke organisatie die AI inzet – en dankzij de EU AI Act nu ook een wettelijke verplichting.

05

AI-governance in de praktijk brengen

De Digitale Overheid (2025) benadrukt dat organisaties een toereikend niveau van AI-geletterdheid moeten bevorderen. Belangrijk hierbij is dat het gewenste niveau niet voor iedereen hetzelfde is; het hangt sterk af van de context waarin AI wordt toegepast, zoals de sector en het type werkzaamheden.

Om AI-geletterdheid praktisch te implementeren, begin je met een grondige inventarisatie van je AI-omgeving. Dit betekent niet alleen het in kaart brengen van formele AI-systemen, maar ook van de alledaagse AI-tools die medewerkers gebruiken, zoals ChatGPT, Microsoft Copilot of AI-gestuurde zoekfuncties. Deze 'verborgen' AI-toepassingen vormen vaak een onderschat risico binnen organisaties. Wanneer je alle AI-toepassingen binnen jouw organisatie identificeert, ze categoriseert volgens de vier risiconiveaus van de AI Act en bepaalt welke systemen onder jouw directe verantwoordelijkheid vallen heb je een solide basis voor alle verdere stappen.

Vervolgens implementeer je gedifferentieerde training die aansluit bij verschillende rollen binnen jouw organisatie. Besluitvormers moeten inzicht krijgen in wat AI kan en niet kan, en welke governance-structuren noodzakelijk zijn. IT-professionals hebben diepere kennis nodig van technische vereisten en beveiligingsimplicaties. En eindgebruikers moeten begrijpen hoe ze op verantwoorde wijze met AI-systemen omgaan in hun dagelijkse werk. Daarbij is het essentieel om specifieke aandacht te besteden aan medewerkers die publiek toegankelijke AI-tools zoals chatbots en generatieve AI gebruiken. Ze moeten begrijpen welke bedrijfsinformatie veilig gedeeld kan worden, hoe ze de output kritisch kunnen beoordelen, en hoe ze de risico's van hallucinerend gedrag en inherente vooroordelen kunnen herkennen.

De laatste stap is het integreren van AI-geletterdheid in bestaande processen. Neem AI-risico's op in je huidige risicoanalyses zoals je ISMS of DPIA's. Voeg AI-specifieke controles toe aan uw beveiligingsbeleid. En verwerk AI-geletterdheid in jouw inkoopvoorwaarden, bijvoorbeeld door een verplichte gebruiksaanwijzing te eisen bij aanschaf van nieuwe AI-systemen. Door deze integratie wordt AI-governance een natuurlijk onderdeel van uw bestaande compliance-raamwerk in plaats van een losstaand project.

Checklist voor AI-compliance binnen uw bestaande frameworks

Framework	AI-integratiepunten	Praktische maatregelen
ISO 27001:2022	• Informatiebeveiligingsrisico's • Vertrouwelijkheid, integriteit, beschikbaarheid	• Voeg AI-specifieke risico's toe aan uw SoA • Implementeer toegangscontrole voor AI-modellen en datasets
NIS2	• Cyberbeveiligingscapaciteiten • Incidentmeldingen	• Specificeer AI-incidenten in uw responsprocedures • Zorg voor 24-uurs meldcapaciteit
AVG/GDPR	• Rechtmatigheid van verwerking • Uitlegbaarheid	• Documenteer verwerkingsdoeleinden voor AI-systemen • Implementeer procedures voor uitlegbaarheid
SOC 2 Type II	• Betrouwbaarheid van diensten • Trust service principles	• Audit uw AI-systemen op betrouwbaarheid • Zorg voor adequate privacy-controles
Dagelijks AI-gebruik	• Acceptabel gebruik van AI-tools • Databescherming bij externe AI-diensten	• Ontwikkel beleid voor gebruik van publieke AI-tools • Creëer richtlijnen voor welke informatie wel/niet gedeeld mag worden

06 Smart learning als brug naar compliance

Om organisaties te helpen bij het verhogen van AI-geletterdheid en het waarborgen van compliance met relevante wet- en regelgeving, hebben wij een unieke aanpak ontwikkeld. Deze combineert de Serious Training methode met praktijkgerichte training en risico-inventarisatie. Deze aanpak vormt de brug tussen theoretische kennis en praktische toepassing, precies wat nodig is in het complexe veld van AI-governance.

Serious Training in de praktijk
Onze Serious Training methode maakt complexe onderwerpen zoals AI-geletterdheid en compliance niet alleen begrijpelijk, maar ook boeiend. Deze innovatieve aanpak onderscheidt zich door:

1. **Realistische simulaties:** Deelnemers worden ondergedompeld in levensechte scenario's door middel van Serious gaming & Gamification waarin ze leren hoe ze onder druk de juiste beslissingen nemen. Ze ervaren hoe het is om met AI-risico's om te gaan vóórdat deze werkelijkheid worden in hun organisatie.
2. **Actief leren:** Door interactieve elementen worden deelnemers gestimuleerd om actief deel te nemen en kennis direct toe te passen. Geen passieve kennisoverdracht, maar een dynamisch leerproces dat beklijft.
3. **Concrete toepassing:** Abstracte concepten zoals de vier risiconiveaus van de AI Act worden vertaald naar praktische situaties die direct relevant zijn voor security- en compliance-professionals. Dit maakt complexe regelgeving toegankelijk en implementeerbaar.
4. **Samenwerking bevorderen:** Deelnemers leren van elkaar door samen uitdagingen aan te gaan en oplossingen te bedenken. Deze collectieve intelligentie versterkt niet alleen het leerproces, maar bereidt teams ook voor op effectieve samenwerking bij werkelijke AI-incidenten.

Deze methode heeft zich bewezen als effectief instrument om organisaties door de complexe wereld van AI-compliance te navigeren, zonder dat iedereen een AI-expert hoeft te worden.

Maatwerk expertise voor elke rol binnen uw organisatie
Onze modulair opgebouwde trainingsprogramma's passen zich naadloos aan bij de diverse functies binnen uw organisatie. De basismodule AI-geletterdheid vormt het fundament voor iedereen die met AI-systemen in aanraking komt. Daarnaast bieden we gerichte verdieping voor specifieke rollen: besluitvormers krijgen inzicht in governance-structuren en strategische implementatie, terwijl IT-professionals zich verdiepen in de technische aspecten van AI-beveiliging en compliance. Voor juridische en compliance-professionals ontwikkelden we een module die zich richt op de praktische vertaling van complexe wet- en regelgeving naar werkbare procedures binnen uw organisatie. Daarnaast bieden we gerichte training voor dagelijkse gebruikers van AI-tools. Deze module richt zich op praktische vaardigheden zoals het effectief formuleren van prompts, het kritisch evalueren van AI-gegenereerde output, en het waarborgen van informatiebeveiliging bij het gebruik van externe AI-diensten.

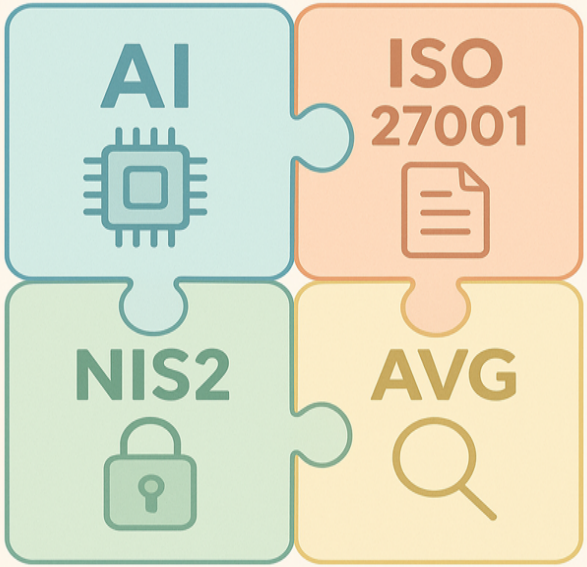
Risico-inventarisatie als solide fundament
Een grondige AI-risico-inventarisatie vormt de basis van onze trainingsaanpak. In nauwe samenwerking met jouw team brengen we eerst alle AI-systemen binnen de organisatie zorgvuldig in kaart. Vervolgens classificeren we de bijbehorende risico's volgens de categorieën van de EU AI Act. Dit stelt ons in staat om precies vast te stellen waar jouw organisatie mogelijk nog niet voldoet aan de nieuwe vereisten. Op basis van deze analyse ontwikkelen we doelgerichte actieplannen met concrete stappen om volledige compliance te bereiken en geïdentificeerde risico's effectief te mitigeren.

07

Voorsprong door slimme integratie

AI-geletterdheid is niet langer een optionele vaardigheid, maar een wettelijke verplichting onder de EU AI Act. "Nu het aantal AI-systemen binnen organisaties sterk toeneemt, wordt AI-geletterdheid belangrijker. Het opbouwen van kennis door je organisatie biedt een bepaalde bescherming aan medewerkers en stimuleert tegelijkertijd de verantwoorde inzet van AI", aldus de Digitale Overheid (2025).

Dit geldt niet alleen voor complexe AI-systemen die uw organisatie implementeert, maar ook voor de alledaagse AI-tools die medewerkers gebruiken in hun dagelijkse werkzaamheden. Door iedereen bewust te maken van zowel de mogelijkheden als de beperkingen van deze tools, minimaliseert u risico's en maximaliseert u tegelijkertijd de productiviteitsvoordelen die deze technologieën bieden.



De unieke Serious Training methode van Smart Training Center biedt een effectieve manier om medewerkers op alle niveaus voor te bereiden op de uitdagingen en kansen van AI. Door realistische simulaties, praktijkgerichte training en grondige risico-inventarisatie combineert deze aanpak alle elementen die nodig zijn voor verantwoorde AI-implementatie.

De basis van effectieve AI-governance is niet het creëren van een geheel nieuw compliance-domein, maar het integreren van AI-risico's en -controles in uw bestaande frameworks. De EU AI Act is bewust opgezet als aanvulling op bestaande regelgeving, met een risicogebaseerde benadering die direct aansluit bij de security- en compliance-methoden die u al gebruikt.

In een wereld waarin AI steeds belangrijker wordt, is het verhogen van AI-geletterdheid niet alleen een compliance-vereiste, maar ook een strategische investering in de toekomst van jouw organisatie.

08

Referenties

1. Digitale Overheid. (2025, februari 26). Wat je moet weten over AI-geletterdheid. Geraadpleegd van https://www.digitaleoverheid.nl/achtergrondartikelen/wat-je-moet-weten-over-ai-geletterdheid/
2. Digitale Overheid. (2025, januari 21). AI-verordening. Geraadpleegd van https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nieuwe-technologieen-data-en-ethiek/artificiele-intelligentie-ai/ai-verordening/
3. European Commission. (2024). The AI Act: The first-ever legal framework on AI. Geraadpleegd van https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
4. Autoriteit Persoonsgegevens. (2024). AI & Algorithmic Risks Report Netherlands – Summer 2024.
5. Lumenova. AI Literacy and Risk Mitigation. Geraadpleegd van https://www.lumenova.ai/blog/ai-literacy-ai-risks
6. IAPP. Beyond Compliance: The Case for Adaptive AI Governance. Geraadpleegd van https://iapp.org/news/a/beyond-compliance-the-case-for-adaptive-ai-governance
7. Frontiers in Human Dynamics. Black Box AI and Compliance Challenges. Geraadpleegd van https://www.frontiersin.org/articles/10.3389/fhumd.2024.1421273/full
8. European Commission. (2024). Digital Economy and Society Index (DESI). Brussel: European Commission.

Plan een adviesgesprek in met Curtis, Maarten en Roeland

Heeft uw organisatie de volgende stap nodig

in AI-geletterdheid en compliance?

Neem direct contact met ons op via 06 4303 0577 of plan een vrijblijvend gesprek in.

Curtis
info@complianceshield.nl

Maarten
Maarten@smarttrainingcenter.eu

roeland
roeland@smarttrainingcenter.eu

Samen brengen we uw AI-governance naar een hoger niveau.

Disclaimer

Deze whitepaper is bedoeld voor algemene informatiedoeleinden en vormt geen professioneel advies. Smart Training Center streeft naar actuele en correcte informatie, maar garandeert geen volledigheid of juistheid. Gebruik van de informatie is op eigen risico.

Raadpleeg altijd een deskundige voor advies dat past bij uw situatie. Smart Training Center is niet aansprakelijk voor schade voortvloeiend uit het gebruik van deze whitepaper.

Door deze whitepaper te gebruiken, stemt u in met deze disclaimer.