

Wie bestuurt de AI in uw organisatie?

Waarom bestuurders zicht en bewijs nodig hebben over AI-gebouwde en
AI-gedreven applicaties

Editie

1 · Oktober 2026

Peildatum

8 oktober 2026

Voor

Bestuur en directie · IT, security en compliance

Wetgeving

AVG · ePrivacy · AI Act · NIS2 (NL, BE, DE) · CRA · Data Act · PLD · DORA · EAA

Kernboodschap

AANTOONBAARHEID

1

Kerncijfers

49–78%

van werknemers gebruikt AI-tools die de werkgever niet heeft goedgekeurd

51%

koppelt AI-tools aan werksystemen zonder goedkeuring van IT

Persoonlijk

aansprakelijk: bestuurders in NL, BE en DE onder de NIS2-wetgeving

€35M / 7%

maximale AI Act-boete (verboden praktijken, wereldwijde omzet)

€20M / 4%

maximale AVG-boete

24 uur

eerste melding bij NIS2-incident en bij misbruikte kwetsbaarheid (CRA, sinds 11 sept. 2026)

Bronnen bij de cijfers: zie hoofdstuk 3 (onderzoek 2025–2026) en hoofdstuk 11.

Managementsamenvatting

AI zit inmiddels in bijna elke applicatie die uw organisatie gebruikt: in zelfgebouwde tools, in ingekochte SaaS en in agents die zelfstandig taken uitvoeren. Een groot deel daarvan is nooit door inkoop, security of compliance gegaan.

Medewerkers kiezen hun eigen tools, koppelen ze aan bedrijfssystemen en bouwen in een middag een applicatie met AI. Tegelijk is de wet veranderd. Sinds de NIS2-omzetting in Nederland, België en Duitsland is cyberveiligheid een bestuurstaak met persoonlijke aansprakelijkheid. De AI Act, de AVG, de Cyber Resilience Act, de Data Act en de nieuwe productaansprakelijkheid leggen daar elk eigen plichten bovenop.

KERNBEVINDING: al die wetten vragen hetzelfde: **aantoonbaarheid**. Weet welke AI er draait, wie de eigenaar is, welke data erin gaat en wat het systeem doet. Beleid op papier en een spreadsheet zijn daarvoor niet genoeg: applicaties veranderen wekelijks, AI-modellen worden vervangen en leveranciers voegen ongemerkt AI-functies toe. Bestuurders hebben daarom een AI-governancetool nodig die doorlopend registreert, bewijs verzamelt en rapporteert.

Deze whitepaper legt uit waarom, welke wetten er spelen en waaraan zo'n tool minimaal moet voldoen. Deel A is geschreven voor bestuur en directie, deel B voor IT, security en compliance.

DEEL A · VOOR BESTUUR EN DIRECTIE

2

Het voorval

In het najaar van 2026 sprak de auteur met een verantwoordelijke bij een beursgenoteerde ICT-organisatie met activiteiten in Nederland en België. Een commercieel team gebruikte daar een signal-based go-to-market-platform: software die koopsignalen verzamelt uit websitebezoek, LinkedIn-activiteit en baanwisselingen, en die toont welke individuele beslisser “warm” is.

Uit de openbare informatie van de leverancier bleek het volgende:

- het platform levert intentiedata op **persoonsniveau**, over mensen die geen klant zijn;
- het koppelt aan tools die LinkedIn-accounts van medewerkers automatisch laten connecten en berichten sturen, terwijl LinkedIn dat in zijn gebruiksvoorwaarden verbiedt;
- het gebruikt AI om personen te scoren, zonder dat zichtbaar is welke modellen of subverwerkers daarachter zitten.

Niemand had kwade bedoelingen. Het team wilde sneller verkopen, en de tool deed wat hij beloofde. Maar de organisatie bleef zelf verwerkingsverantwoordelijke onder de AVG, gebruiksverantwoordelijke onder de AI Act en, als essentiële of belangrijke entiteit, verantwoordelijk voor haar toeleveringsketen onder NIS2.

De vraag die de verantwoordelijke stelde, is de kern van deze whitepaper: **hoe weten wij als bestuur welke AI-applicaties er in onze organisatie draaien, en of we kunnen aantonen dat ze mogen?**

De casus is geanonimiseerd. Organisatie en leverancier worden niet genoemd.

3

De wildgroei

Het voorval is geen uitzondering. Recente onderzoeken laten hetzelfde beeld zien.

Bevinding	Bron
49% van werknemers in organisaties met 500+ medewerkers gebruikt niet-goedgekeurde AI-tools; 51% koppelt AI-tools aan werksystemen zonder IT	BlackFog, januari 2026
52% van kenniswerkers gebruikt niet-goedgekeurde AI; 58% van bestuurders meldt een AI-gerelateerd securityincident in de afgelopen 12 maanden	Okta, AI Agents at Work 2026
78% van Amerikaanse werknemers gebruikt niet-goedgekeurde AI; slechts 7,5% kreeg uitgebreide AI-training	WalkMe (SAP), augustus 2025
In IT en telecom gebruikt 73% schaduw-AI, terwijl 84% de risico's kent	TrustedTech, september 2026

Drie vormen van wildgroei

- 1. **Zelfgebouwd met AI.** Medewerkers en teams bouwen applicaties met AI-codeerassistenten en no-codeplatforms. Wat vroeger een IT-project van maanden was, staat nu in een middag live, vaak zonder review, testomgeving of eigenaar.
- 2. **Ingekochte SaaS met AI.** Bestaande leveranciers voegen AI-functies toe aan software die al jaren in gebruik is. Het contract, de verwerkersovereenkomst en de risicoanalyse dateren van vóór die AI.
- 3. **AI-agents.** Systemen die zelfstandig beslissen, berichten sturen of data verwerken, met rechten in meerdere applicaties tegelijk.

Opvallend is het gat tussen bestuur en werkvloer: bestuurders denken zicht te hebben, terwijl meer dan de helft van de medewerkers eigen tools gebruikt. **Juist dat gat maakt de bestuurder kwetsbaar.**

4 Bestuurdersaansprakelijkheid in de EU

Cyberveiligheid is geen IT-onderwerp meer, maar een plicht van het bestuur, en die plicht is niet te delegeren. Artikel 20 van de NIS2-richtlijn verplicht elke lidstaat om ervoor te zorgen dat bestuursorganen de beveiligingsmaatregelen goedkeuren, op de uitvoering toezien, training volgen en aansprakelijk kunnen worden gesteld bij inbreuken. Elk EU-land heeft dit in een eigen wet omgezet.

Land	Nationale wet	Wat het betekent voor bestuurders
Nederland	Cyberbeveiligingswet (Cbw), van kracht sinds 15 augustus 2026	Zorgplicht en opleidingsplicht voor het bestuur; persoonlijke aansprakelijkheid bij verwaarlozing; toezichthouders kunnen een bestuurder onder omstandigheden tijdelijk schorsen
België	NIS2-wet van 26 april 2024, van kracht sinds 18 oktober 2024	Het bestuursorgaan keurt de maatregelen goed, ziet toe en kan aansprakelijk worden gesteld; toezicht door het CCB
Duitsland	NIS2-Umsetzungsgesetz, van kracht sinds 6 december 2025	§ 38 BSIG: de Geschäftsleitung moet de maatregelen uitvoeren en bewaken, is persoonlijk aansprakelijk voor schade bij plichtsverzuim en heeft een trainingsplicht
Overige EU	Nationale NIS2-wet	Dezelfde kern uit art. 20 NIS2, nationaal ingevuld

Daarnaast geldt het gewone vennootschapsrecht: onbehoorlijke taakvervulling (art. 2:9 BW in Nederland, art. 2:56 WVV in België, § 93 AktG en § 43 GmbHG in Duitsland). Wie als bestuurder geen zicht heeft op AI-applicaties met persoonsgegevens of toegang tot kritieke systemen, kan zich moeilijk beroepen op onwetendheid.

Drie andere wetten vergroten de druk

- **AVG art. 5(2).** De organisatie moet de naleving kunnen aantonen; de bewijslast ligt bij haar.

- **AI Act.** De gebruiksverantwoordelijke heeft eigen plichten, zoals AI-geletterdheid (art. 4, sinds februari 2025) en transparantie (art. 50, sinds augustus 2026).
- **Beursnotering.** Het jaarverslag beschrijft de voornaamste risico's en de interne beheersing. Een structureel gat in AI-governance hoort daarin thuis, en wordt door toezichthouders, accountants en beleggers gelezen.

DEEL B · VOOR IT, SECURITY EN COMPLIANCE

5

Heatmap: welke wet raakt welke AI-applicatie

Verordeningen gelden direct en gelijk in alle EU-lidstaten. Richtlijnen worden per land omgezet, waardoor naam, toezichthouder en details verschillen. Hieronder de inschatting van de impact per soort applicatie.

Impact: ●●● hoog ●● midden ● laag

Wet	Van toepassing	Zelf-ge-bouwd	SaaS met AI	AI-agents	Kern voor AI-applicaties
AVG	Verordening, sinds 2018	●●●	●●●	●●●	Grondslag, profilering, DPIA, verwerkers-overeenkomst, doorgifte buiten de EER
ePrivacy	Richtlijn, nationaal om-gezet	●●	●●●	●●	Toestemming voor tracking en bezoekers-identificatie
AI Act	Verordening; art. 4 sinds feb. 2025, art. 50 sinds aug. 2026, hoog risico vanaf dec. 2027	●●●	●●	●●●	Rol (aanbieder of gebruiksverantwoordelij-ke), AI-geletterdheid, transparantie, risico-klasse
NIS2	Richtlijn; NL 15 aug. 2026, BE 18 okt. 2024, DE 6 dec. 2025	●●	●●●	●●●	Ketenbeveiliging, incidentmelding, bestuurs-verantwoordelijkheid
Cyber Resilience Act	Verordening; meldplicht sinds 11 sept. 2026, vol-ledig 11 dec. 2027	●●●	●●	●●	Wie software op de markt brengt, is fabri-kant: security-by-design, kwetsbaarheden melden binnen 24 uur
Data Act	Verordening, sinds 12 sept. 2025	●	●●●	●●	Overstappen tussen clouddiensten, datapor-tabiliteit, geen lock-in
Product-aansprakelijkheid (PLD)	Richtlijn 2024/2853; pro-ducten op de markt van-af 9 dec. 2026	●●●	●●	●●	Software en AI vallen expliciet onder pro-ductaansprakelijkheid
DORA	Verordening, sinds 17 jan. 2025 (financiële sec-tor)	●●	●●●	●●	ICT-derdenrisico, register van ICT-dienstver-leners

European Accessibility Act

Richtlijn, sinds 28 juni 2025



Toegankelijkheid van digitale diensten voor consumenten

De kolom **zelfgebouwd met AI** springt eruit. Wie met AI een applicatie bouwt en die aan klanten of partners levert, kan onder de CRA fabrikant worden en onder de nieuwe productaansprakelijkheid aansprakelijk zijn voor gebreken, ook als de code door een AI-assistent is geschreven.

6

Financiële blootstelling

Boetes zijn maxima; toezichthouders wegen ernst, duur, verwijtbaarheid en medewerking. Toch laat een rekenvoorbeeld zien hoe snel de blootstelling oploopt wanneer één AI-applicatie meerdere wetten tegelijk raakt.

Voorbeeld: een beursgenoteerde organisatie met € 5 miljard wereldwijde jaaromzet en een ongecontroleerde AI-applicatie die personen profileert.

Wet	Maximum	Toegepast op € 5 mld omzet
AVG (art. 83(5))	€ 20 mln of 4%	tot € 200 mln
AI Act, transparantie en overige plichten (art. 99(4))	€ 15 mln of 3%	tot € 150 mln
NIS2, essentiële entiteit	€ 10 mln of 2%	tot € 100 mln

De boetes zijn de zichtbare kosten. Minstens zo zwaar wegen:

- schadeclaims van betrokkenen, ook collectief (zoals onder de Nederlandse WAMCA);
- herstelkosten: data verwijderen, processen stilleggen, systemen vervangen;
- geblokkeerde accounts en verloren commerciële kanalen;
- reputatieschade en vragen van aandeelhouders en commissarissen;
- persoonlijke aansprakelijkheid en mogelijke schorsing van bestuurders.

Rekenvoorbeeld ter illustratie; boetes worden per overtreding en per toezichthouder vastgesteld.

7

Waarom beleid en spreadsheets niet volstaan

Veel organisaties hebben een AI-beleid en een lijst met goedgekeurde tools. Dat is een goed begin, maar het beantwoordt de vraag van de toezichthouder niet: *laat zien wat er werkelijk draait, en sinds wanneer*.

- **Een lijst verouderd op de dag dat hij klaar is.** Applicaties krijgen wekelijks updates, leveranciers wisselen van AI-model en medewerkers voegen zelf tools toe.
- **Beleid zegt wat mag, niet wat er gebeurt.** Het bewijs moet uit de systemen zelf komen: welke versie draaide, welk model, welke data, wie gaf goedkeuring.
- **Bewijs moet terugwerkend te leveren zijn.** Bij een incident of klacht wil de toezichthouder weten hoe de situatie was op het moment zelf, niet hoe die er nu uitziet.
- **De keten is groter dan de organisatie.** Subverwerkers, AI-modellen en integraties van derden vallen onder dezelfde verantwoordelijkheid.
- **Meerdere wetten, één set feiten.** AVG, AI Act, NIS2 en CRA vragen deels hetzelfde bewijs. Wie per wet een apart dossier bijhoudt, doet het werk vier keer en raakt het overzicht kwijt.

Governance verschuift daarmee van een **jaarlijkse vragenlijst** naar een **doorlopend systeem** dat registreert, meet en rapporteert.

8

Wat een AI-governancetool minimaal moet kunnen

Ongeacht leverancier of oplossing: dit zijn de functies die een bestuurder nodig heeft om aan de wetten in deze whitepaper te kunnen voldoen.

Functie	Wat het doet	Waarom (wettelijke basis)
Register	Overzicht van alle AI-applicaties, agents en AI-functies in SaaS, met eigenaar, doel en status	AVG art. 30, AI Act (rolbepaling), NIS2 art. 21
Classificatie	Rol en risicoklasse per applicatie: aanbieder of gebruiksverantwoordelijke; verboden, hoog risico, transparantie of minimaal	AI Act art. 5, 6, 50
Data- en ketenzicht	Welke persoonsgegevens, welke subverwerkers, welke AI-modellen, waar opgeslagen	AVG art. 28, 35, 44 e.v.; NIS2 art. 21(2) (d); DORA
Versie- en gebruiks-bewijs	Vastleggen welke versie, welk model en welke instructies op welk moment draaiden, met een controleerbaar spoor	AVG art. 5(2), AI Act logging, CRA

Goedkeuring en controls	Wie keurde wat goed, welke maatregelen gelden, welke uitzonderingen zijn verleend	NIS2 art. 20; Cbw-zorgplicht; § 38 BSIG
Incidenten en kwetsbaarheden	Signaleren en registreren, met termijnen van 24 en 72 uur	NIS2 art. 23, CRA art. 14, AVG art. 33
Bestuursrapportage	Periodiek overzicht voor bestuur en raad van commissarissen of toezicht, met trend en open risico's	NIS2 art. 20, jaarverslag
Herbeoordeling	Automatisch signaal bij een nieuwe leverancier, een nieuw model of een nieuwe AI-functie	AI Act, AVG art. 35(11), Data Act (overstappen)

Twee eisen gelden voor de tool zelf. Hij moet **onafhankelijk** meten in plaats van te vertrouwen op wat een applicatie over zichzelf meldt. En hij moet **licht** te starten zijn: een organisatie moet binnen weken een eerste register en baseline hebben, niet na een project van maanden.

9

Zeven patronen uit de praktijk

1. **“Het is maar een marketingtool.”** Commerciële tools verwerken vaak meer persoonsgegevens dan kernsystemen, en vallen buiten de radar van security.
2. **De proefperiode wordt productie.** Een gratis trial met echte klantdata wordt stilzwijgend de werkwijze, zonder contract of verwerkersovereenkomst.
3. **AI sluipt binnen via een update.** Een bestaande leverancier voegt AI toe; de oude risicoanalyse blijft in de kast liggen.
4. **De bouwer is ook de keurder.** Wie een applicatie met AI bouwt, test en keurt hem vaak zelf goed. Onafhankelijke controle ontbreekt.
5. **Geen eigenaar.** Bij een incident blijkt niemand verantwoordelijk voor de applicatie, het model of de data.
6. **Bewijs achteraf reconstrueren.** Pas bij een klacht of audit wordt gezocht naar wat er draaide. Dan blijkt het spoor er niet te zijn.
7. **Het bestuur hoort het als laatste.** Risico's blijven hangen bij IT of het team, terwijl de wet de verantwoordelijkheid juist bij het bestuur legt.

10

Zelftest voor bestuurders

Kunt u elk van deze vragen vandaag beantwoorden, met bewijs?

- ☐ Weten wij welke AI-applicaties, AI-agents en AI-functies in SaaS er in onze organisatie in gebruik zijn?
- ☐ Heeft elke AI-applicatie een eigenaar die verantwoordelijk is voor gebruik, data en risico?
- ☐ Weten wij per applicatie welke persoonsgegevens worden verwerkt en welke AI-modellen en subverwerkers daarachter zitten?
- ☐ Hebben wij voor profilerende of risicovolle toepassingen een DPIA?
- ☐ Weten wij per applicatie of wij aanbieder of gebruiksverantwoordelijke zijn onder de AI Act, en in welke risicoklasse?
- ☐ Kunnen wij aantonen welke versie en welk model op een bepaald moment draaiden?
- ☐ Brengen wij zelfgebouwde AI-software op de markt, en voldoen wij dan aan de CRA en de nieuwe productaansprakelijkheid?
- ☐ Worden nieuwe AI-tools getoetst voordat ze met bedrijfssystemen worden gekoppeld?
- ☐ Hebben bestuurders de verplichte cybersecuritytraining gevolgd, en is dat vastgelegd?
- ☐ Krijgt het bestuur periodiek een rapportage over AI-risico's, met open punten en trend?

Zes of meer keer “nee” of “weet ik niet” betekent dat de bewijslast die de wet bij u legt, vandaag niet te dragen is.

11

Bronnen

Wetgeving

- [AVG, Verordening \(EU\) 2016/679](#)
- [AI Act, Verordening \(EU\) 2024/1689](#) en [Digital Omnibus on AI, Verordening \(EU\) 2026/1744](#)
- [NIS2, Richtlijn \(EU\) 2022/2555](#)
- [Cyber Resilience Act, Verordening \(EU\) 2024/2847](#)
- [Data Act, Verordening \(EU\) 2023/2854](#)
- [Productaansprakelijkheid, Richtlijn \(EU\) 2024/2853](#)
- [DORA, Verordening \(EU\) 2022/2554](#)
- [Cyberbeveiligingswet \(NL\), toelichting CMS](#)
- [Belgische NIS2-wet, toelichting Lexgo](#)
- [Duitse NIS2-omzetting, § 38 BSIG, toelichting Taylor Wessing](#)
- [CRA-tijdlijn, Crowell](#)

- [LinkedIn: verboden software en extensies](#)

Onderzoek schaduw-AI (2025–2026)

- [BlackFog Shadow AI Research](#)
- [Okta, AI Agents at Work 2026 \(The Register\)](#)
- [WalkMe \(SAP\), AI in the Workplace Survey 2025](#)
- [TrustedTech \(IT Brief\)](#)

Mike Hes

Oprichter, HES Consultancy International

Mike Hes heeft meer dan dertig jaar ervaring in ICT. HES Consultancy International (Arnhem, KvK 89821009) helpt organisaties en leveranciers met EU-regelgeving, compliance en markttoegang. hes-consultancy-international.com

Informatief document, geen juridisch advies. Laat de toepassing op uw organisatie toetsen door uw juridische adviseur. Peildatum: 8 oktober 2026 (Editie 1). © 2026 HES Consultancy International.