56. AI: een onmiskenbare taak van het bestuur

MR. S.F. TER BRAKE & MR. DRS. H.S. KLEINJAN

Op grond van hun vennootschapsrechtelijke taken, de AVG, de AI-verordening en de NIS2-richtlijn moeten besturen fundamentele keuzes maken over het gebruik van AI, organisatie-inrichting, verantwoordelijkheidsverdeling en risicobeheersing. Elke bestuurder is verantwoordelijk voor de inzet en het gebruik van AI door de vennootschap en moet daarom in meer of mindere mate kennis van AI hebben.

Inleiding

Artificial Intelligence (AI) kan op steeds meer manieren worden ingezet en raakt daarom steeds vaker aan kernprocessen en besluitvorming binnen ondernemingen. Dit stelt bestuurders voor nieuwe vragen over kennis, verantwoordelijkheid en aansprakelijkheid. Dit artikel zal verkennen of en in hoeverre bestuurders van Nederlandse vennootschappen[1] kennis moeten hebben en rekenschap moeten geven van AI, gezien hun vennootschapsrechtelijke taken en de daaruit voortvloeiende normen, alsmede aan AI gerelateerde wet- en regelgeving, zoals de Algemene Verordening Gegevensbescherming (AVG),[2] de AI-verordening[3] en de NIS2-richtlijn.[4][5]

Wat wordt verstaan onder AI?

Artificial Intelligence (AI), ofwel kunstmatige intelligentie, is een verzamelbegrip voor technologie die systemen in staat stelt om, voor expliciete of impliciete doelstellingen, uit invoergegevens af te leiden hoe output te genereren, zoals voorspellingen, aanbevelingen, inhoud of beslissingen, die invloed kunnen hebben op fysieke of virtuele omgevingen.[6] De systemen waarin dergelijke technologie wordt toegepast, kunnen verschillen in de mate van autonomie en aanpassingsvermogen. Daaronder kan ook geautomatiseerde besluitvorming worden begrepen, waarbij beslissingen of beslissingsondersteuning door technologische middelen plaatsvinden, al dan niet met menselijke tussenkomst.

Een belangrijk deelgebied binnen AI is *machine learning*, dat betrekking heeft op algoritmen die op basis van gegevens patronen leren herkennen en op basis daarvan output genereren. *Deep learning* vormt een specifieke vorm van *machine learning* waarbij gebruik wordt gemaakt van meerlagige neurale netwerken, die met name geschikt zijn voor de verwerking van complexe en ongestructureerde gegevens.

1 Wij beperken ons in dit artikel tot vennootschappen. De inhoud van dit artikel zal grotendeels hetzelfde zijn voor andere rechtspersonen.

2 Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende ede bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG, PB L 119/1, 4.5.2016 (Algemene Verordening Gegevensbescherming/ AVG).

3 Verordening (EU) 2024/1689 van het Europees Parlement en de Raad van 13 juni 2024 tot vaststelling van geharmoniseerde regels inzake artificiele intelligentie, PB L, 2024/1689, 12.7.2024 (AI-verordening).

4 Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148, PB L 333, 27.12.2022 (NIS2-richtlijn).

5 Bestuurdersaansprakelijkheid (zowel intern als extern) valt derhalve buiten het bereik van dit artikel.

6 In internationale beleidskaders wordt dit begrip meestal benaderd aan de hand van het AI-systeem waarin deze technologie is belichaamd, een benadering die ook is overgenomen in de AI-verordening. Vgl. OECD, Explanatory Memorandum on the Updated OECD Definition of an AI System (OECD Artificial Intelligence Papers, maart 2024), waarin de in november 2023 vastgestelde definitie is toegelicht; zie tevens art. 3 onder 1 AI-verordening.

Bedrijven zetten AI-toepassingen,[7] veelal gebaseerd op *machine learning*-technieken, steeds vaker in voor toepassingen zoals fraudedetectie en risicoselectie, aanbevelingssystemen, klantenservice en toepassingen in sectoren als gezondheidszorg en logistiek, waarbij de mate van volwassenheid en opschaling per toepassing kan verschillen.[8] Ook verkennen steeds meer bedrijven het gebruik van *AI-agents*, zij het voornamelijk in experimentele of pilotomgevingen. Dit zijn systemen die zelfstandig meerdere stappen uitvoeren, beslissingen nemen en andere tools aansturen.[9]

AI-beleid en -strategie

Het bestuur is belast met het besturen van de vennootschap.[10] Kerntaken van het bestuur zijn het ontwikkelen van het beleid en de strategie van de vennootschap en de met haar verbonden onderneming. Bij de vervulling van hun taak moeten bestuurders zich richten naar het belang van de vennootschap en de met haar verbonden onderneming, welk vooral wordt bepaald door het bevorderen van het bestendige succes van de door de vennootschap gedreven onderneming.[11] In de Nederlandse Corporate Governance Code staat dat het bestuur verantwoordelijk is voor de continuïteit en duurzame langetermijnwaardecreatie van de vennootschap en de met haar verbonden onderneming.[12] Hoewel de Nederlandse Corporate Governance Code slechts van toepassing is op beursvennootschappen, gelden de principes van deze code als breedgedragen algemene opvattingen over goede *corporate governance* en geven zij invulling aan de open norm van behoorlijk bestuur zoals vervat in art. 2:9 BW.

De vraag of en in hoeverre een onderneming gebruik zal gaan maken van AI is een strategische vraag en behoort derhalve tot het bestuursdomein. De snelle ontwikkeling van AI, de voorziene impact daarvan op het bedrijfsleven en de vereiste langetermijnvisie van het bestuur maken onzes inziens dat elk bestuur zich deze vraag ook zou moeten stellen. Het antwoord op de vraag of en in hoeverre een onderneming gebruik zal gaan maken van AI zal uiteraard afhangen van verschillende factoren, zoals de bedrijfsactiviteiten van de vennootschap en de daarmee samenhangende kansen en risico's voor de vennootschap.

De snelle ontwikkeling van AI, de voorziene impact daarvan op het bedrijfsleven en de vereiste langetermijnvisie van het bestuur maken onzes inziens dat elk bestuur zich deze vraag zou moeten stellen

Als AI voor een onderneming kansen biedt, maar het bestuur kiest ervoor om hier niets mee te doen, dan ontstaat het risico dat de onderneming wordt voorbijgestreefd door concurrenten die deze kansen wel benutten. Gesteld zou kunnen worden dat een dergelijke keuze niet is gericht op bestendig succes. Uiteraard moet een vennootschap wel de financiële middelen hebben om te kunnen investeren in AI. Hoever bestuurders moeten gaan in het aantrekken van financiering voor AI-investeringen hangt onzes inziens af van het effect dat AI kan hebben op de bedrijfsactiviteiten en de continuïteit van de onderneming.

Bij de vervulling van hun taak moeten bestuurders zorgvuldig omgaan met de belangen van alle stakeholders, waaronder aandeelhouders en klanten.[13] Dat betekent dat investeringen in en het gebruik van AI op een zo efficiënt en verantwoord mogelijke manier moeten worden gedaan. Concrete vragen die het bestuur zich daarom bij het opstellen van het AI-beleid en de strategie dient te stellen zijn:

i. Welke AI-toepassingen zijn het meest geschikt voor de onderneming en hoe kunnen deze het beste worden toegepast?
ii. Zijn er voldoende beschikbare en geschikte data?
iii. Welke eisen stelt de onderneming aan betrouwbaarheid en uitlegbaarheid van AI-toepassingen alvorens deze als basis voor besluitvorming worden gebruikt?
iv. Welke aanpassingen in bedrijfsprocessen, structuren en werkwijzen zijn nodig om AI succesvol te implementeren?
v. Hoe wordt binnen de onderneming het AI-beleid uitgewerkt en aangestuurd, inclusief verantwoord gebruik en wie daarbij de eindverantwoordelijkheid voor toezicht, besluitvorming en verantwoording draagt?

7 In dit artikel gebruiken wij de term AI-toepassingen als een praktische en leesbare verzamelnaam voor alles wat in de dagelijkse praktijk als 'AI' wordt ervaren. Juridisch gezien hanteert de AI-verordening echter een andere terminologie en spreekt primair over AI-systemen: het geheel van software, technische componenten, processen en organisatorische maatregelen dat met behulp van kunstmatige intelligentie tot bepaalde uitkomsten komt. Het AI-systeem is daarmee het centrale aanknopingspunt voor regelgeving, verantwoordelijkheden en toezicht. Aan de basis van elk AI-systeem liggen één of meer AI-modellen. Dit zijn de getrainde algoritmen die patronen herkennen, voorspellingen doen of beslissingen ondersteunen. Hoewel modellen de technische kern vormen, functioneren zij in de praktijk altijd binnen een breder systeem en worden zij juridisch vooral relevant in specifieke contexten, zoals bij *general-purpose* AI. Wanneer in dit artikel wordt gesproken over AI-toepassingen, wordt daarmee dus het volledige geheel bedoeld: de zichtbare toepassing voor de gebruiker, het onderliggende AI-systeem in juridische zin en de gebruikte AI-modellen als technische basis. Deze terminologische keuze dient uitsluitend de leesbaarheid en doet geen afbreuk aan de juridische kwalificatie van deze technologieën.

8 Vgl. Autoriteit Persoonsgegevens, *Rapportage AI & Algoritmes Nederland*, maart 2026; *Europese Commissie, Apply AI Strategy – Shaping Europe's digital future*, 8 oktober 2025; McKinsey & Company, *The State of AI: Global Survey 2025*, 5 november 2025.

9 Vgl. McKinsey Global Institute, *Agents, robots, and us: Skill partnerships in the age of AI*, november 2025, waarin AI-agents worden beschreven als systemen die niet-fysieke taken autonoom kunnen uitvoeren en steeds vaker worden ingezet als onderdeel van heringerichte *workflows* waarin mensen, *agents* en robots samenwerken.

10 Art. 2:129/art. 239 BW.

11 HR 4 april 2014, ECLI:NL:HR:2014:797, «JOR» 2014/290, *NJ* 2014/286, m.nt. Van Schilfgaarde (*Cancun*).

12 Nederlandse Corporate Governance Code 2025, Principe 1.1.

13 Asser/Van Solinge & Nieuwe Weme *2-IIb* 2019/128.

vi. Hoe wordt de naleving van geldende wet- en regelgeving (zoals de AVG en de AI-verordening) geborgd?
vii. Welke gevolgen heeft de inzet van AI voor medewerkers, organisatiecultuur en de vereiste kennis en vaardigheden?
viii. Wat zijn de risico's van het gebruik van AI voor de onderneming en haar stakeholders?

Risicomanagement

AI brengt niet alleen kansen, maar ook risico's met zich mee. Het gebruik van AI kan leiden tot beperkte transparantie, onder meer wanneer wordt gewerkt met zogenoemde *black box*-modellen waarvan de besluitvorming moeilijk te reconstrueren is. Dit geldt in het bijzonder voor systemen die gebruikmaken van *deep learning*, waarbij uitkomsten worden gegenereerd op basis van statistische patronen in grote datasets.
Daarnaast bestaat het risico op bias en discriminatie, bijvoorbeeld wanneer trainingsdata historische ongelijkheden weerspiegelen en deze door het systeem worden gereproduceerd of versterkt. Ondernemingen zoals personeelsdienstverleners, banken en verzekeraars moeten daarom extra waarborgen nemen om te voorkomen dat het gebruik van AI tot discriminatie zal leiden.
Ook kan onduidelijkheid ontstaan over verantwoordelijkheid en aansprakelijkheid, met name bij inzet van (semi-) autonome systemen zoals *AI-agents*. Bij generatieve AI[14] doen zich bovendien specifieke risico's voor, zoals het produceren van onjuiste of misleidende informatie (hallucinaties), het schenden van auteursrechten en het vergemakkelijken van misbruik, waaronder *deepfakes* en grootschalige desinformatie. De schaalbaarheid van AI vergroot daarbij de potentiële impact van fouten of onrechtmatige beslissingen aanzienlijk.
Het vaststellen en beperken van risico's is eveneens een belangrijke bestuurstaak.[15] In de Nederlandse Corporate Governance Code is hierover opgenomen dat de vennootschap over adequate interne risicobeheersings- en controlesystemen moet beschikken. Daaraan wordt toegevoegd dat het bestuur de risico's die verbonden zijn aan de strategie en de bedrijfsactiviteiten moet inventariseren en analyseren. In de toelichting wordt specifiek gewezen op de risico's verbonden aan nieuwe technologieën en veranderende businessmodellen, zoals op het gebied van ethisch verantwoorde toepassing van nieuwe technologieën, bijvoorbeeld Responsible AI.[16, 17]
De precieze vereisten die aan risicobeheersings- en controlesystemen mogen worden gesteld, zijn afhankelijk van de aard, omvang, complexiteit en levensfase van de onderneming, gebruiken binnen de branche en de aard van de risico's.[18] Ondernemingen die met persoonsgegevens werken, zullen bovendien extra alert moeten zijn op het waarborgen van privacy en het voorkomen van datalekken. Recent waarschuwde de Autoriteit Persoonsgegevens voor het delen van gevoelige informatie met chatbots naar aanleiding van een toenemend aantal meldingen van datalekken gerelateerd aan het gebruik van AI-chatbots zoals ChatGPT, Claude en Gemini.[19]
Meer concreet menen wij dat het bestuur de volgende waarborgen dient in te bouwen ter beheersing van juridische, ethische, operationele, reputatie-, duurzaamheids- en geopolitieke risico's verbonden aan AI:
i. Het voorkomen van vooroordelen en discriminatie, onder meer door het tegengaan van bias in ontwikkelteams en in trainingsdata.
ii. Het borgen van de kwaliteit en betrouwbaarheid van AI-toepassingen teneinde systeemfouten als gevolg van gebrekkige programmering en onvolledige of inadequaat beheerde datasets te voorkomen.
iii. Het nemen van passende technische en organisatorische maatregelen ter beperking van cyberveiligheidsrisico's zoals onbevoegde toegang tot en onrechtmatig gebruik van data, *hacking*, *malware* en manipulatie van AI-toepassingen, teneinde schending van privacy en vertrouwelijkheid te voorkomen.
iv. Het behouden van voldoende transparantie en uitlegbaarheid van AI-toepassingen, zodat effectief toezicht, controle en juridische verantwoording mogelijk zijn.
v. Het stellen van duidelijke kaders voor het gebruik van AI ter voorkoming van taakoverschrijding en besluitvorming buiten het beoogde toepassingsgebied, inclusief het beleggen van verantwoordelijkheid en aan-

14 'Generatieve AI' is het deelgebied van AI dat gebruikmaakt van *deep learning*, getraind op grote datasets, om nieuwe content te creëren, zoals geschreven tekst, code, afbeeldingen, muziek, simulaties en video's. Generatieve AI genereert nieuwe output op basis van bestaande data, in plaats van uitsluitend voorspellingen te doen over nieuwe gegevens.
15 Art. 2:141/art. 251 lid 2 BW; Asser/Nieuwe Weme & Salemink *2-IIb* 2025/139.
16 Responsible AI verwijst naar een op de principes uit de Key Terms for AI Governance gebaseerde benadering van de ontwikkeling en governance van AI, waaronder onder meer de beginselen van beveiliging, veiligheid, transparantie, uitlegbaarheid, verantwoordelijkheid, privacy en non-discriminatie of het voorkomen van vooringenomenheid (bias). De term 'Responsible AI' komt niet letterlijk voor in de AI Act, maar de onderliggende principes zijn duidelijk verankerd in de verordening. Zie o.a. overwegingen 6, 20 en 27 van de AI-verordening waarin het belang van mensgerichte, betrouwbare en ethisch verantwoorde AI wordt benadrukt. Dit vertaalt zich naar verplichtingen rond transparantie, menselijk toezicht, veiligheid, non-discriminatie, privacy en verantwoordingsplicht.
17 Nederlandse Corporate Governance Code 2025, Best Practice 1.2.1.
18 D.A.M.H.W. Strik, *Aansprakelijkheid voor een falend risicomanagement. Preadvies van de Vereniging Handelsrecht*, Deventer: Kluwer 2010, p. 275.
19 *Het Financieele Dagblad*, 'Privacywaakhond waarschuwt voor datalekken door AI-gebruik', 29 december 2025. Zie ook eerdere berichtgeving op de website van de AP, *Let op: gebruik AI-chatbot kan leiden tot datalekken*, Autoriteit Persoonsgegevens, 6 augustus 2024.

sprakelijkheid voor schade die kan ontstaan door het gebruik van (semi-)autonome AI-toepassingen.[20]

vi. Het nemen van voorzieningen ter waarborging van de continuïteit van de onderneming bij onjuiste adviezen, storingen of uitval van AI-toepassingen.

vii. Waarborgen ten aanzien van externe leveranciers en partners, met inachtneming van geopolitieke ontwikkelingen en de locatie van data en infrastructuur, ter waarborging van adequate controle, duidelijke verantwoordelijkheden en continuïteit binnen de AI-keten.[21]

De werking van deze waarborgen kan onder meer gecontroleerd worden door stresstesten, de vorm waarvan zal worden bepaald op basis van de bedrijfsactiviteiten van de vennootschap.[22]

Naleving van en verantwoordelijkheden onder AI-gerelateerde wetgeving

Het bestuur is ervoor verantwoordelijk dat de vennootschap de op haar van toepassing zijnde wet- en regelgeving naleeft.[23] Dit geldt uiteraard ook voor de aan AI gerelateerde wet- en regelgeving, zoals de AVG, AI-verordening en NIS2.

AVG: rechtmatigheid, transparantie en dataminimalisatie

Zodra AI-systemen worden ingezet waarbij persoonsgegevens worden verwerkt, geldt onverkort het kader van de AVG. Dit brengt onder meer verplichtingen mee ten aanzien van rechtmatigheid, transparantie, dataminimalisatie, en passende technische en organisatorische maatregelen. Daarnaast moeten de regels inzake profilering, geautomatiseerde besluitvorming en Data Protection Impact Assessments (DPIA's) worden nageleefd. De AVG richt zich tot de verwerkingsverantwoordelijke en kent geen expliciete norm voor bestuurders, maar vergt naleving die niet zonder besluitvorming en borging op bestuursniveau kan plaatsvinden.

AI-verordening; governanceverplichtingen

Op 1 augustus 2024 is de Europese AI-verordening in werking getreden met een gefaseerde toepassing.[24] De AI-verordening is van toepassing op natuurlijke personen, rechtspersonen of overheidsinstanties binnen en buiten de EU die AI-systemen[25] voor de Europese markt ontwikkelen, importeren of distribueren, integreren in een product of toepassen in hun bedrijfsvoering. Daarmee raakt de AI-verordening in de praktijk een groot deel van het bedrijfsleven en de publieke sector.

Een onderscheid wordt gemaakt tussen aanbieder[26] en gebruiksverantwoordelijken van AI-systemen.[27] Hoewel de meest vergaande verplichtingen alleen gelden voor aanbieders van AI-systemen[28] is dit onderscheid voor bestuurders minder geruststellend dan het lijkt. Gebruiksverantwoordelijken kunnen van kleur verschieten naar aanbieder, bijvoorbeeld als zij een AI-systeem ingrijpend wijzigen of het systeem onder eigen naam aanbieden.[29] Bestuurders zullen daarom moeten begrijpen welke rol de vennootschap feitelijk vervult bij de inzet van AI.

Centraal in de AI-verordening staat een risicogebaseerde benadering, waarin AI-systemen worden ingedeeld naar hun potentiële impact op mens en maatschappij. Welke specifieke verplichtingen gelden, hangt daarom af van de risicoclassificatie van het AI-systeem dat wordt ontwikkeld, geïmporteerd, gedistribueerd, geïntegreerd of toegepast. Dit betekent dat niet elke AI-toepassing dezelfde aandacht vergt, maar wel dat organisaties moeten weten welke AI-systemen zij gebruiken en in welke risicocategorie deze vallen.

Bij AI-systemen met een beperkt risico gelden in principe uitsluitend transparantieverplichtingen. Aanbieders moeten waarborgen dat AI-interactie en AI-gegenereerde content

20 Het voorstel voor de AI Liability Directive (Richtlijn inzake aansprakelijkheid voor artificiële intelligentie), COM(2022) 496, dat beoogde de civielrechtelijke aansprakelijkheid bij schade door AI-systemen te harmoniseren, is inmiddels door de Europese Commissie ingetrokken wegens het ontbreken van voldoende politiek draagvlak. Daarmee blijft de civielrechtelijke aansprakelijkheid voor schade door AI-systemen voorlopig hoofdzakelijk op nationaal niveau geregeld, binnen de kaders van het bestaande Europese productaansprakelijkheidsrecht en valt verder buiten de reikwijdte van deze bijdrage.

21 Zie ook deels S.W. van der Ven, 'De veranderende taak van bestuurders in het tijdperk van AI', in: *MvO* 2020/7, p. 196-197.

22 Idem.

23 K.H.M. de Roo, 'De nalevingsplicht van het bestuur van rechtspersonen', in: *Ondernemingsrecht* 2018/2.

24 De eerste verboden gelden sinds februari 2025, terwijl de kernverplichtingen voor hoog-risico-AI in beginsel vanaf 2 augustus 2026 van toepassing zijn. Het Digitale Omnibus-voorstel van november 2025 biedt daarbij ruimte voor beperkt uitstel, maar laat onverlet dat organisaties nu al moeten starten met de inrichting van beleid, processen en toezicht.

25 Een AI-systeem wordt in art. 3 van de AI-verordening gedefinieerd als een op een machine gebaseerd systeem dat is ontworpen om met verschillende niveaus van autonomie te werken en dat na het inzetten ervan aanpassingsvermogen kan vertonen, en dat, voor expliciete of impliciete doelstellingen, uit de ontvangen input afleidt hoe output te genereren zoals voorspellingen, inhoud, aanbevelingen of beslissingen die van invloed kunnen zijn op fysieke of virtuele omgevingen.

26 'Aanbieder' wordt in art. 3 van de AI-verordening gedefinieerd als een natuurlijke of rechtspersoon, overheidsinstantie, agentschap of ander orgaan die/dat een AI-systeem of een AI-model voor algemene doeleinden ontwikkelt of laat ontwikkelen en dat systeem of model in de handel brengt of het AI-systeem in gebruik stelt onder de eigen naam of merk, al dan niet tegen betaling.

27 'Gebruiksverantwoordelijke' wordt in art. 3 van de AI-verordening gedefinieerd als een natuurlijke of rechtspersoon, overheidsinstantie, agentschap of ander orgaan die/dat een AI-systeem onder eigen verantwoordelijkheid gebruikt, tenzij het AI-systeem wordt gebruikt in het kader van een persoonlijke niet-beroepsactiviteit.

28 Art. 16 AI-verordening.

29 Art. 25 AI-verordening. Zie ook V.G. Lam & L.M. Bredschneijder, 'Contractuele risicobeperking in de AI waardeketen. De "beschouwde aanbieder" volgens artikel 25 van de Europese AI verordening', *Contracteren* 2025/1, p. 18-19.

als zodanig herkenbaar zijn, terwijl gebruiksverantwoordelijken betrokkenen moeten informeren bij de inzet van emotieherkenning, biometrische categorisering of *deepfakes*.[30] Verdere rapportage-, registratie- of beheersverplichtingen volgen uit de AI-verordening in beginsel niet.

Voor hoog-risico-AI-systemen[31] gelden strikte verplichtingen. Het gaat daarbij om toepassingen die worden ingezet in contexten waarin de uitkomsten of ondersteuning van besluitvorming aanzienlijke gevolgen kunnen hebben voor personen en hun grondrechten. Voorbeelden zijn AI-systemen die worden gebruikt bij personeelsbeslissingen, zoals selectie, promotie of beëindiging van arbeidsrelaties, maar ook systemen die een rol spelen bij besluiten over toegang tot essentiële publieke of private diensten, zoals uitkeringen, leningen of verzekeringen. Dit zijn toepassingen die ook in de reguliere ondernemingspraktijk aan de orde kunnen zijn.

De meeste materiële verplichtingen ten aanzien van hoog-risico-AI-systemen rusten op de aanbieder van het systeem.[32] Aanbieders moeten beschikken over een doorlopend risicobeheerssysteem dat de gehele levenscyclus van het AI-systeem bestrijkt, aangevuld met eisen aan data-governance,[33] waaronder de kwaliteit, relevantie en representativiteit van trainings-, validatie- en testdata. Bovendien gelden er eisen ten aanzien van technische documentatie, transparantie en menselijk toezicht, alsmede waarborgen inzake nauwkeurigheid, robuustheid en cyberbeveiliging van de hoog-risico-AI-systemen.[34] Daarnaast dienen aanbieders te beschikken over een passend kwaliteitsbeheerssysteem, zorg te dragen voor automatische *logging*, alsmede zo nodig corrigerende maatregelen te treffen.[35] Na ingebruikname zijn aanbieders verplicht het functioneren te monitoren en incidenten en tekortkomingen te melden.[36][37]

Gebruiksverantwoordelijken op hun beurt dienen passende technische en organisatorische maatregelen te treffen voor een zorgvuldige en rechtmatige inzet van hoog-risico-AI-systemen. Deze verplichtingen omvatten onder meer het borgen van menselijk toezicht, het gebruik van het AI-systeem overeenkomstig de door de aanbieder verstrekte instructies, het monitoren van de werking van het systeem gedurende de gebruiksfase en voor zover zij daarover controle hebben het waarborgen van de relevantie en representativiteit van de gebruikte inputdata.[38] In de praktijk vergt dit een duidelijke interne borging, bijvoorbeeld in de vorm van beleid of richtlijnen voor het verantwoord gebruik van AI, waarin is vastgelegd hoe AI wordt ingezet, wie waarvoor verantwoordelijk is en wanneer escalatie of ingrijpen is aangewezen.

Toepassingen met een onaanvaardbaar risico zijn verboden. Dit betreft de zogenaamde verboden AI-praktijken,[39] waaronder AI-systemen die de vrije keuze van mensen beperken of manipuleren, of die een ernstige aantasting van grondrechten meebrengen. Hieronder vallen onder meer bepaalde vormen van *social scoring*, *predictive policing*, emotieherkenning in werk- en onderwijscontexten en specifieke toepassingen van gezichts- en biometrische technologie. Ook dit onderstreept dat bestuurders zicht moeten hebben op welke AI-toepassingen binnen de vennootschap worden gebruikt en waar duidelijke grenzen liggen.

De AI-verordening veronderstelt dat organisaties hun inzet van AI bewust en systematisch inventariseren en afbakenen

De AI-verordening richt zich primair op de regulering van AI-systemen als product en op de verplichtingen van aanbieders en gebruiksverantwoordelijken. Zij bevat geen expliciete bepalingen over verantwoordelijkheid of aansprakelijkheid van bestuurders. Niettemin brengt de verordening verplichtingen mee die besluitvorming en aansturing op bestuursniveau veronderstellen. Zij moeten de inzet van AI bewust en systematisch inventariseren en afbakenen. Besturen zullen zich rekenschap moeten geven van de inzet van AI binnen de vennootschap, de daaraan verbonden risico's en de wijze waarop toezicht en interventie zijn georganiseerd. De AI-verordening legt sterke nadruk op menselijk toezicht en vereist dat AI-systemen zodanig worden ontworpen en ingezet dat effectieve interventie door mensen mogelijk blijft.[40] Deze verplichting impliceert niet alleen technische

30 Art. 50 AI-verordening.

31 Art. 6 en bijlage III AI-verordening.

32 De meeste verplichtingen ten aanzien van hoog-risico-AI-systemen rusten op de aanbieder van het systeem, vgl. art. 16 AI-verordening.

33 Dit is een benaming voor het in kaart brengen en beheersen van risico's, zie J. Armour & H. Eidenmueller, 'Self driving-corporations', in *ECGI Working Paper* nr. 475/2019, p. 91. Zie tevens art. 9 (systeem voor risicobeheer) en art. 10 (data en datagovernance) AI-verordening.

34 Art. 8-15 AI-verordening zoals art. 11 (technische documentatie), art. 13 (transparantie en informatieverstrekking), art. 14 (menselijk toezicht) en art. 15 (nauwkeurigheid, robuustheid en cyberbeveiliging) AI-verordening.

35 Art. 16-21 AI-verordening.

36 Art. 72 en 73 AI-verordening inzake post-market monitoring en incidentmeldingen.

37 Voordat een hoog-risico-AI-systeem in de handel wordt gebracht of in gebruik wordt gesteld, moet de toepasselijke conformiteitsbeoordelingsprocedure zijn doorlopen. Na afronding daarvan stellen aanbieders een EU-conformiteitsverklaring op, brengen zij de CE-markering aan en registreren zij het AI-systeem in de EU-database voor hoog-risico-AI-systemen. Zie art. 43 (conformiteitsbeoordelingsprocedure), art. 47-48 (EU-conformiteitsverklaring en CE-markering) en art. 49 (EU-database voor hoog-risico-AI-systemen) AI-verordening.

38 Voor de zelfstandige verplichtingen van gebruiksverantwoordelijken van hoog-risico-AI-systemen zie met name art. 26 AI-verordening, gelezen in samenhang met art. 4 (AI-geletterdheid), art. 14 (menselijk toezicht), art. 27 (grondrechten-impactbeoordeling, waar van toepassing) en art. 49 (registratie) AI-verordening.

39 Art. 5 AI-verordening.

40 Art. 14 AI-verordening (menselijk toezicht). Menselijk toezicht is onder de AI-verordening vooral een expliciete en bindende verplichting voor AI-systemen met een hoog risico. Voor andere AI-systemen kan menselijke betrokkenheid indirect vereist zijn op grond van transparantieverplichtingen of andere rechtskaders, zoals de AVG.

maatregelen, maar ook organisatorische borging: wie is bevoegd in te grijpen, onder welke omstandigheden en met welke verantwoordelijkheden?

Daarnaast moeten aanbieders en gebruiksverantwoordelijken van AI-systemen ervoor zorgen dat betrokken medewerkers beschikken over voldoende kennis en vaardigheden om AI verantwoord toe te passen.[41] De Autoriteit Persoonsgegevens heeft deze norm nader geconcretiseerd in haar handreiking over AI-geletterdheid,[42] waarin een praktisch vierstappenmodel wordt gehanteerd: identificeren, doelen stellen, uitvoeren en evalueren. AI-geletterdheid is een continu structureel proces, geen eenmalige *compliance*-actie.[43]

Interessant is dat de Autoriteit Persoonsgegevens AI-geletterdheid expliciet koppelt aan bestuurlijke betrokkenheid. In de praktijk krijgt dit thema volgens de AP vaak een bottom-upinvulling, maar zonder duidelijke top-downsturing blijft de aanpak versnipperd en onvoldoende geborgd. Bestuurders van vennootschappen die met AI-systemen werken, moeten daarom zelf beschikken over voldoende inzicht in de werking, risico's en kansen van AI om richting te kunnen geven aan verantwoord gebruik en om effectief toezicht te houden op de naleving van wet- en regelgeving. De Autoriteit Persoonsgegevens benadrukt in dit verband dat agendering op bestuurlijk niveau essentieel is en dat AI-geletterdheid geen losstaand initiatief mag zijn, maar onderdeel dient uit te maken van een bredere AI-strategie of -visie.

NIS2-richtlijn: expliciete bestuurlijke verantwoordelijkheid

De NIS2-richtlijn,[44] die in Nederland naar verwachting in 2026 zal worden geïmplementeerd[45] in de Cyberbeveiligingswet (Cbw), is van toepassing op publieke en private entiteiten die als essentiële of belangrijke entiteit kwalificeren en actief zijn in de in de richtlijn aangewezen sectoren, waaronder energie, transport, digitale infrastructuur, zorg, drinkwater- en afval(water)beheer, post- en koeriersdiensten, de productie van kritieke producten en bepaalde digitale diensten.[46] De NIS2-richtlijn heeft tot doel de digitale weerbaarheid en cyberbeveiliging van organisaties te versterken en verplicht organisaties die onder haar toepassingsbereik vallen om passende maatregelen te treffen ter bescherming van hun netwerken en informatiesystemen tegen risico's zoals cyberaanvallen, datalekken en systeemuitval. Een belangrijk kenmerk van de NIS2-richtlijn is dat de verantwoordelijkheid hiervoor expliciet bij het managementorgaan wordt gelegd. De NIS2-richtlijn verplicht lidstaten te waarborgen dat leden van het managementorgaan van essentiële en belangrijke entiteiten aansprakelijk kunnen worden gehouden voor inbreuken van de entiteit op de richtlijnverplichtingen, overeenkomstig het nationale recht.[47] In Nederland wordt hieraan invulling gegeven via het bestaande bestuursrechtelijke en civielrechtelijke kader.[48] Bestuursleden zijn bovendien verplicht om door middel van opleidingen de nodige kennis en vaardigheden te verwerven om cyberrisico's en de impact daarvan te kunnen beoordelen. Het wetsvoorstel Cbw voorziet, naast handhaving jegens de entiteit, expliciet in persoonlijke bestuursrechtelijke handhaving jegens individuele bestuurders. Op grond van het wetsvoorstel Cbw kan aan een bestuurslid een last onder dwangsom of bestuurlijke boete worden opgelegd bij niet-naleving van de in het wetsvoorstel neergelegde kennis en scholingsverplichtingen.[49]

41 Art. 4 AI-verordening. Zie ook Europese Commissie, Voorstel voor een verordening van het Europees Parlement en de Raad tot wijziging van Verordeningen (EU) 2024/1689 en (EU) 2018/1139 wat betreft de vereenvoudiging van de toepassing van geharmoniseerde regels inzake artificiele intelligentie (Digital Omnibus on AI), COM(2025) 836 final, 2025/0359, Brussel, 19 november 2025. In de Digital Omnibus on AI wordt geconstateerd dat de huidige formulering van art. 4 AI-verordening, waarin aanbieders en gebruiksverantwoordelijken worden aangesproken op AI-geletterdheid, in de praktijk leidt tot onzekerheid over de reikwijdte van deze verplichting. Om die reden stelt de Commissie voor de bepaling te herformuleren, zodat niet langer een ongespecificeerde nalevingsplicht voor individuele organisaties centraal staat, maar een expliciete opdracht aan de Commissie en de lidstaten om AI-geletterdheid systematisch te bevorderen. De opleidingsverplichtingen voor gebruiksverantwoordelijken van hoog-risico-AI blijven daarbij onverkort gelden.

42 Autoriteit Persoonsgegevens, *Verder bouwen aan AI-geletterdheid. Een kernvoorwaarde voor verantwoorde AI*, Den Haag: AP, oktober 2025.

43 Handreikingen en richtsnoeren van de Autoriteit Persoonsgegevens hebben geen juridisch bindende status, maar gelden als *soft law*. Uit de rechtspraak van het Hof van Justitie blijkt dat de uitleg van nationale toezichthouders niet zonder meer bindend is voor de rechtstoepassing, zoals geïllustreerd in HvJ EU 4 oktober 2024, ECLI:EU:C:2024:858 (*KNLTB*).

44 De NIS2-richtlijn en zie tevens wetsvoorstel Regels ter implementatie van Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (*PbEU* 2022, L 333) (wetsvoorstel Cyberbeveiligingswet), *Kamerstukken II* 2024/25, 36764, nr. 2.

45 Ten tijde van het schijven van dit artikel is het wetsvoorstel Cyberbeveiligingswet (*Kamerstukken II* 2024/25, 36764) nog in behandeling bij de Tweede Kamer; voor 16 maart 2026 staat een wetgevingsoverleg van de vaste commissie voor Digitale Zaken gepland. De Cyberbeveiligingswet treedt in werking nadat de Tweede en Eerste Kamer akkoord hebben gegeven. Naar verwachting is dat Q2 2026, maar dat hangt af van wanneer de behandeling in de Kamers is en de vraag is of dat nog realistisch is.

46 De toepasselijkheid van de NIS2-richtlijn is daarbij in beginsel beperkt tot middelgrote en grote entiteiten, behoudens expliciete uitzonderingen, zie art. 20 NIS2-richtlijn (bestuurlijke verantwoordelijkheid en aansprakelijkheid), alsmede art. 32 en 34 NIS2 inzake toezicht en sancties.

47 Art. 20 NIS2-richtlijn.

48 Zie *Kamerstukken II* 2024/25, 36764, nr. 3 (MvT), p. 44-45.

49 Zie o.a. art. 20, art. 32 en art. 34 NIS2-richtlijn. In het wetsvoorstel Cyberbeveiligingswet dat strekt tot implementatie van deze bepalingen in Nederland, zijn deze verantwoordelijkheden o.a. uitgewerkt in art. 24 wetsvoorstel Cbw (bestuurlijke verantwoordelijkheid en scholing), art. 78 Cbw (verzoek tot schorsing bestuur) en art. 92-93 wetsvoorstel Cbw (handhaving en sancties jegens leden van het bestuur).

Hoewel de NIS2-richtlijn niet specifiek op AI ziet, vallen veel AI-gerelateerde risico's door hun digitale aard indirect onder het toepassingsbereik ervan.[50] Daarmee vullen NIS2 en de AI-verordening elkaar onzes inziens aan: de AI-verordening richt zich op inhoudelijke waarborgen rond het gebruik van AI, terwijl de NIS2-richtlijn de bestuurlijke verantwoordelijkheid voor digitale weerbaarheid en risicobeheersing expliciteert.

Delegatie en taakverdeling

Het bepalen of en op welke manier AI het beste in de onderneming kan worden ingezet, alsmede in hoeverre en op welke manier AI het beste kan worden gecontroleerd, is een steeds complexere en belangrijkere taak van het bestuur.[51] Dit vergt specifieke, technische en analytische kennis en vaardigheden van de bestuurders. Door de snelle en recente opkomst van AI bezitten veel bestuurders deze kennis en vaardigheden nog niet.

> Een belangrijk kenmerk van de NIS2-richtlijn is dat zij de verantwoordelijkheid hiervoor expliciet bij het managementorgaan legt. De Cyberbeveiligingswet voorziet, in aanvulling op handhaving jegens de entiteit, expliciet in persoonlijke bestuursrechtelijke handhaving jegens individuele bestuurders

Vennootschappen die in belangrijke mate gebruikmaken van AI, of waar het gebruik van AI grote risico's met zich meebrengt, hebben vaak al de nodige kennis in huis of kunnen overwegen om een specifieke AI-functionaris aan te stellen. Echter, het bestuur blijft verantwoordelijk voor het risicomanagement van de vennootschap, waaronder de zorg voor adequate beheers- en controlesystemen voor het gebruik van AI. Dit betekent dat de bestuurders de AI-functionaris moeten controleren. Om de AI-functionaris te kunnen controleren, moeten de bestuurders in zekere mate zelf ook AI-geletterd zijn. Zij zouden daarvoor trainingen kunnen volgen die de ethische, technische en juridische aspecten van AI-systemen onder de loep nemen.[52]

Bovendien moeten zij zich goed door de AI-functionaris laten informeren om de door de vennootschap gebruikte AI-systemen te begrijpen.

Het bestuur zou ook kunnen overwegen om een specialistische bestuurder aan te trekken, of een van de huidige bestuurders de 'AI-taak' toe te bedelen. Dit ontslaat de overige bestuurders echter niet van hun verantwoordelijk hiervoor. Op grond van art. 2:9 lid 2 BW draagt elke bestuurder namelijk verantwoordelijkheid voor de algemene gang van zaken. In de literatuur wordt aangenomen dat onder de algemene gang van zaken worden verstaan aangelegenheden die van wezenlijke betekenis zijn voor de vennootschap, zoals het algemene beleid en de strategie, de financiën, het risicobeleid en belangrijke transacties.[53] Zoals in hiervoor uiteengezet, is het gebruik van AI onderdeel van het algemene beleid en de strategie, alsmede van het specifieke risicobeleid. Dit betekent dat de overige bestuurders zich niet kunnen disculperen van aansprakelijkheid met een beroep op de taakverdeling.[54] Ook in dit geval moeten bestuurders de met de 'AI-taak' belaste bestuurder dus kunnen controleren, waarvoor zij de werking, het gebruik en de risico's van AI wel eerst moeten begrijpen.

Conclusie

Elk bestuur moet zich de vraag stellen of en in hoeverre de door haar bestuurde vennootschap gebruik zal gaan maken van AI. Om die vraag gefundeerd te kunnen beantwoorden, is een zekere mate van kennis over AI nodig. Indien het antwoord bevestigend is, moet het bestuur een AI-beleid en -strategie opstellen, waarbij de kansen en risico's van AI in kaart worden gebracht en rekening wordt gehouden met de belangen van alle stakeholders, waaronder aandeelhouders en klanten. Vervolgens moet het bestuur zorgdragen voor adequate risicobeheersings- en controlesystemen.

> Ook in dit geval moeten de overige bestuurders de met de 'AI-taak' belaste bestuurder dus kunnen controleren, waarvoor zij de werking, het gebruik en de risico's van AI wel eerst moeten begrijpen

Het bestuur is ervoor verantwoordelijk dat de vennootschap de aan AI gerelateerde wet- en regelgeving naleeft, zoals de AVG, de AI-verordening en de NIS2-richtlijn. Bovendien volgen daaruit ook indirect verplichtingen voor het bestuur. Op grond van de AVG moeten bestuur-

50 Zie ook *Kamerstukken II* 2024/25, 36764, nr. 3 (MvT), p. 86 waarin wordt benoemd dat 'essentiële entiteiten en belangrijke entiteiten moeten bij het maken van hun risicobeoordeling en het treffen van mitigerende maatregelen ook rekening houden met nieuwe technologieën of nieuwe vormen van dreigingen. Dat geldt dus ook voor generatieve kunstmatige intelligentie'.

51 Zie o.m. J. Armour & H. Eidenmueller, 'Self driving-corporations', in *ECGI Working Paper* nr. 475/2019, p. 6 en S.W. van der Ven, 'De veranderende taak van bestuurders in het tijdperk van AI', in *MvO* 2020/7, p. 196.

52 Vgl. Handreiking AP, p. 3.

53 Asser/Nieuwe Weme & Salemink *2-IIb* 2025/177; Wezeman in *Bestuur en Toezicht*; J.B. Huizink, 'Artikel 2:9 BW; enkele observaties', in: J.B. Huizink & J.M. de Jongh e.a. (red.), *Hoe verder met collegiaal bestuur in Nederland?* (ZIFO-reeks Deel I) Deventer: Kluwer 2011, p. 9.

54 Asser/Nieuwe Weme & Salemink *2-IIb* 2025/177.

ders passende technische en organisatorische maatregelen nemen om te zorgen dat sprake is van rechtmatigheid, transparantie en dataminimalisatie bij de verwerking van persoonsgegevens. De AI-verordening impliceert dat de verantwoordelijkheid voor de inrichting, werking en borging van AI-*governance* in belangrijke mate op bestuursniveau behoort te worden belegd. In samenhang bezien leggen de AI-verordening en de NIS2-richtlijn een verplicht normatief *governance*- en risicokader neer dat directe implicaties heeft voor het bestuur.

Ook indien de 'AI-taak' wordt uitbesteed aan een werknemer of wordt toebedeeld aan één bestuurder, dan blijven de overige bestuurders eveneens verantwoordelijk voor de behoorlijke uitoefening van deze taak. Bestuurders kunnen zich niet disculperen met een beroep op de toebedeling van de AI-taak aan een medebestuurder. Bestuurders van ondernemingen die gebruikmaken van AI moeten daarom in zekere mate kennis hebben van AI en AI-geletterd zijn teneinde richting te kunnen geven aan verantwoord gebruik en de inzet van AI op adequate wijze te kunnen beheersen. AI is daarmee niet slechts een *compliance*- of *tech*-onderwerp, maar een *governance*-thema waarvoor bestuurlijke betrokkenheid onmisbaar is.

Dit artikel is afgesloten op 10 maart 2026.

Over de auteurs

Mr. S.F. ter Brake
Advocaat te Amsterdam bij Lexence.

Mr. drs. H.S. Kleinjan
Advocaat te Amsterdam bij Lexence.