

HISCOX
Verzekerd van expertise

# AI en wetgeving: Praktische handvatten voor veilige innovatie

## HISCOX × ICTRECHT

ICTRECHT

Inzicht uit samenwerking. Deze whitepaper is voortgekomen uit een kennissessie tussen Hiscox en ICTRecht

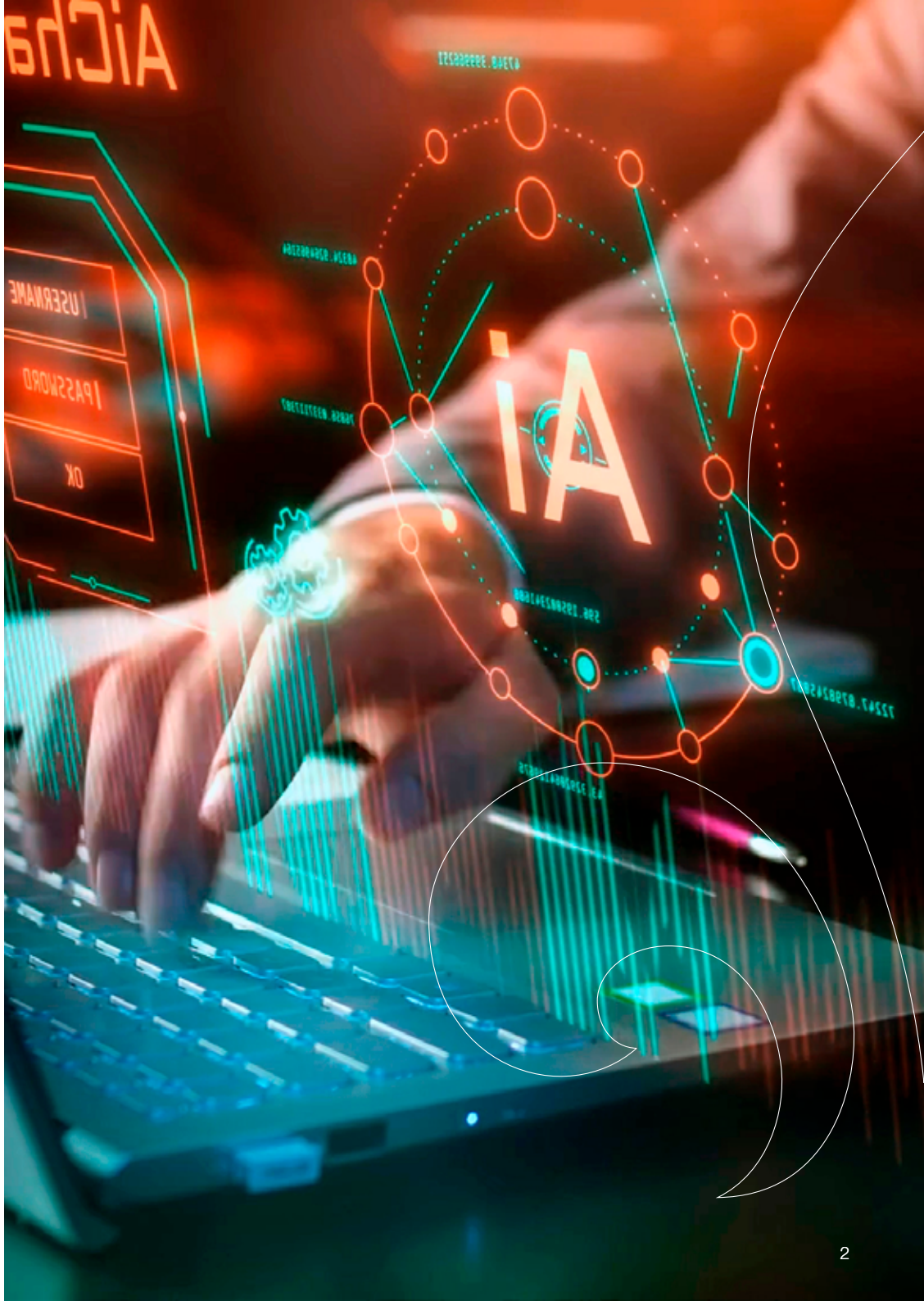
# AI: kansen én risico's onder controle houden

AI is allang geen toekomstmuziek meer. Het zit in zoekmachines, kantoorsoftware, klantenservice, logistiek en zelfs in auto's. Ondernemers in de tech sector benutten AI volop om te innoveren, te schalen en efficiënter te werken. Maar deze vooruitgang brengt ook nieuwe risico's mee: van modelbias en fouten tot deepfakes, fraude en vragen over aansprakelijkheid bij schade.

Met de komst van de AI Act in Europa ontstaat een duidelijker kader voor toezicht en regelgeving. Tegelijk blijven bestaande wetten – zoals de AVG en het civiele aansprakelijkheidsrecht – van kracht. Dit vraagt van ondernemers om AI-activiteiten te classificeren, systemen nauwkeurig te definiëren in contracten en menselijk toezicht organisatorisch te borgen.

Bij Hiscox zien we deze uitdagingen dagelijks. Samen met onze partner ICTRecht bieden we de juridische, operationele en verzekerings-technische expertise die AI-innovaties veilig en compliant houdt. Zo kunnen bedrijven met vertrouwen bouwen aan slimme oplossingen.

*Deze whitepaper bevat specifieke technologische termen. Voor wie daar minder vertrouwd mee is, is achterin een verklarende woordenlijst opgenomen.*



# Wet- en regelgeving rondom AI: kansen en risico's

### 1.1 Van beslisbomen naar generatieve AI

Niet elk geautomatiseerd systeem werkt met AI. Klassieke beslisbomen ('als dit, dan dat') zijn rule-based en volledig transparant. Bij machine learning en deep learning wordt gebruikgemaakt van gewichten en verborgen lagen, waardoor uitkomsten niet altijd direct uitlegbaar zijn. Generatieve AI gaat nog een stap verder: dit type produceert tekst, beeld, audio of video op basis van patronen uit trainingsdata. Hoewel krachtig, is het ook gevoelig voor hallucinaties, bias en uiteenlopende risico's rond intentie en output.

### 1.2 Bias en datakwaliteit

Modellen die leren van internetdata en historische datasets nemen vaak bestaande menselijke vooroordelen over. Dit kan leiden tot verrassende resultaten: een beeldmodel dat 'sneeuw' associeert met 'geiten' omdat alle getrainde geitenfoto's in de sneeuw waren genomen, of een tankdetector die 'bosjes' als vijandelijk beschouwde door de samenhang in trainingsdata. De prestaties van gezichts- en emotieherkenning kunnen aanzienlijk afnemen afhankelijk van de iemands huidskleur. De uitkomst van AI-modellen wordt sterk beïnvloed door de datakwaliteit, representativiteit en context. Zonder goede instructies volgt het model patronen, niet altijd het juiste signaal.

### 1.3 Overredende maar foutieve antwoorden

Grote taalmodellen richten zich op antwoorden die overtuigend en nuttig lijken, maar dat garandeert geen juistheid. Zo kunnen juridische citaten of kenmerken van jurisprudentie 'verzonnen' zijn als het model dergelijke patronen herkent. Zorg daarom altijd voor menselijk toezicht en broncontrole, vooral bij besluiten met verstrekkende juridische of financiële gevolgen. Zekerheid begint bij het zorgvuldig beheren van risico's.

Chatbots zijn getraind om overtuigend en resoluut over te komen. Hierin schuilt het risico dat er toezeggingen worden gedaan namens de organisatie die de chatbot inzet, terwijl dit niet in lijn is met wat de organisatie daadwerkelijk wenst te communiceren.* Het hoogste doel van een chatbot is op dit moment nog het geven van antwoord, niet het geven van een juist antwoord.

* Zo heeft de chatbot van Air Canada een korting toegezegd waar een passagier eigenlijk geen recht op had. De rechter oordeelde dat Air Canada wel degelijk gehouden is aan de toezegging van de chatbot. Zie https://decisions.civilresolutionbc.ca/crt/crtd/en/item/525448/index.do

### 1.4 Deepfakes, synthetische media en fraude

AI kan realistische synthetische content genereren, zoals facturen, schadefoto's en video's. Dit biedt creatieve mogelijkheden, maar verhoogt ook het risico op fraude en reputatieschade. De AI Act introduceert technologische watermerken en labelplichten, bijvoorbeeld bij deepfakes, om dit risico te beperken. Toch kunnen deze controles omzeild worden, bijvoorbeeld door foto's te maken van AI-content. Daarom is aanvullende menselijke toetsing onmisbaar in processen waar dergelijke content als bewijs wordt gebruikt. Dit voorkomt fouten en waarborgt betrouwbaarheid.

Maar afhankelijkheid kan leiden tot deskilling: professionals verliezen signaalgevoeligheid en missen plausibiliteitsfouten. Om dit te beheersen, zijn outcome-verificatie, dubbele controles en samenwerking tussen mens en model essentieel. Dat voorkomt risico's en waarborgt betrouwbare resultaten binnen kritieke processen.

### 1.5 Van chatbots naar agents

AI verschuift van conversatie naar zelfstandige agents die onder andere API's aansturen, interne systemen koppelen of via MCP (Model Context Protocol) toegang krijgen tot informatie. Dit verhoogt de efficiëntie, maar vergroot ook de impact van fouten. Bij koppelingen met systemen zoals EPD's, CRM's of ERP's ontstaan privacy-, integriteits- en continuïteitsrisico's. Met sterk governancebeleid en toegangscontrole worden ongewenste gevolgen voorkomen en wordt het vertrouwen gewaarborgd.

Met deze zelfstandigheid komt ook het menselijk toezicht in het geding. Kan er bij een foutieve handeling van het AI-systeem nog ingegrepen worden? Agents en de bijbehorende mogelijkheden zijn relatief nieuw en gevoelig voor manipulatie en phishing. Dit behoeft extra aandacht. Een voorbeeld hiervan is het plaatsen van teksten op een website die voor mensen niet zichtbaar zijn maar die een agent wel kan herkennen. Op deze manier kunnen opdrachten gegeven worden aan de agent die een mens niet ziet maar wel schadelijke gevolgen kunnen hebben.

# Wet- en regelgeving: nu en straks

**2.1 AI Act in vogelvlucht**

De AI Act is een Europese toezichtswet die een risicogebaseerde benadering hanteert. Hiermee wordt regulering afgestemd op de impact van AI-toepassingen.

- *Verboden praktijken*: Denk aan social scoring, manipulatieve systemen en biometrische categorisering op gevoelige kenmerken. Zorg dat je contractueel vastlegt dat jouw systemen hier niet voor bedoeld of inzetbaar zijn en neem technische maatregelen om dergelijke praktijken te voorkomen.

- *Hoogrisico-systemen*: Dit omvat AI als (onderdeel van een) veiligheidsonderdelen van gereguleerde producten (liften, auto's, luchtvaart, medische hulpmiddelen), maar ook toepassingen die burgers beïnvloeden, zoals systemen voor examenbewaking en beoordeling, triage in de zorg, werving en selectie en het stellen van risico's en prijzen bij zorg- en levensverzekering. Extra eisen zoals transparantie, menselijk toezicht, monitoring en auditing gelden hier.

- *Systemen met een transparantierisico*: systemen die synthetische teksten, afbeeldingen of video maken moeten maatregelen nemen zodat duidelijk is dat het gaat om AI-gegenereerde content. Dit varieert van een visueel watermerk tot technische maatregelen die ervoor moeten zorgen dat gegenereerde content machineleesbaar is. Generatieve AI en tools zoals ChatGPT of Copilot vallen hier onder.

- *Ten slotte* zijn er nog AI-systemen die niet verboden zijn of hoog risico met zich meebrengen en geen transparantierisico hebben. Voor deze systemen gelden beperkte vereisten die met name zien op het bevorderen van AI-geletterdheid. Overigens geldt het vereiste omtrent AI-geletterdheid ook voor de eerder benoemde systemen.

De wet is van toepassing op aanbieders en gebruikers van de AI systemen in de EU, óók als de output alleen in de EU wordt gebruikt. Zorg dus voor duidelijke governance en compliance.



## 2.2 Plichten voor aanbieders en gebruiksverantwoordelijken

Bij het aanbieden en inzetten van hoogrisico-AI-systemen brengt de AI Act duidelijke verplichtingen met zich mee.

*Voor aanbieders*

Wie een AI-systeem onder een eigen naam op de markt brengt, is onder andere verantwoordelijk voor:

- Een kwaliteits- en risicomanagementsysteem met periodieke herbeoordeling. Dit moet proportioneel zijn en mag pragmatisch worden ingericht.
- Uitgebreide documentatie: gebruiksinstructies, doelbinding, beperkingen, prestatie-indicatoren, datasetbeschrijving en validatie.
- Transparantie en uitlegbaarheid, zodat gebruikers beslissingen kunnen verantwoorden tegenover betrokkenen en toezichthouders.
- Data- en modelgovernance met aandacht voor herkomst, rechten, representativiteit en logging.
- Conformiteitsbeoordeling en CE-markering voor markttoegang in de EU.
- Bevordering van AI-geletterheid.

*Voor gebruikers van systemen*

Bedrijven die AI-systemen toepassen, moeten onder andere:

- Controleren of een systeem een CE-markering heeft (en het gebruik staken als dat ontbreekt).
- Menselijk toezicht organiseren dat verder gaat dan standaardchecks, met duidelijke escalatieprocessen.
- Logging en auditability borgen om compliance te waarborgen.
- AI-geletterdheid in het team versterken door beleid, training en toegangsbeheer.

*Let op je rol*

Wie een eigen interface of workflow bouwt boven een model van een derde partij en onder de eigen naam lanceert, word dan gezien als de aanbieder. Zorg dus voor heldere compliance vanaf de start.

### 2.3 Transparantieplichten en watermerken

Communicatie met chatbots moet transparant zijn en duidelijk gemeld worden vóór de eerste interactie. Generatieve content vereist technologische watermerken die machine leesbaar zijn. Voor deepfakes (beeld-, audio- of videomateriaal dat gelijkenis vertoont met bestaande personen, voorwerpen, plaatsen, entiteiten of gebeurtenissen) geldt dat deze expliciete en zichtbare labels moeten bevatten. Volg altijd de gebruikshandleiding en beoordeel de integratie van technische watermerken. Gebruik je een model voor een toepassing die valt onder de transparantieverplichtingen, dan ligt de aansprakelijkheid bij jou als gebruiksverantwoordelijke of integrator. Daarnaast is het belangrijk om na te gaan of er naast de transparantieverplichtingen ook aanvullende verplichtingen zijn, omdat de toepassing kwalificeert als een hoogrisico AI-systeem. Het een sluit het ander namelijk niet uit.

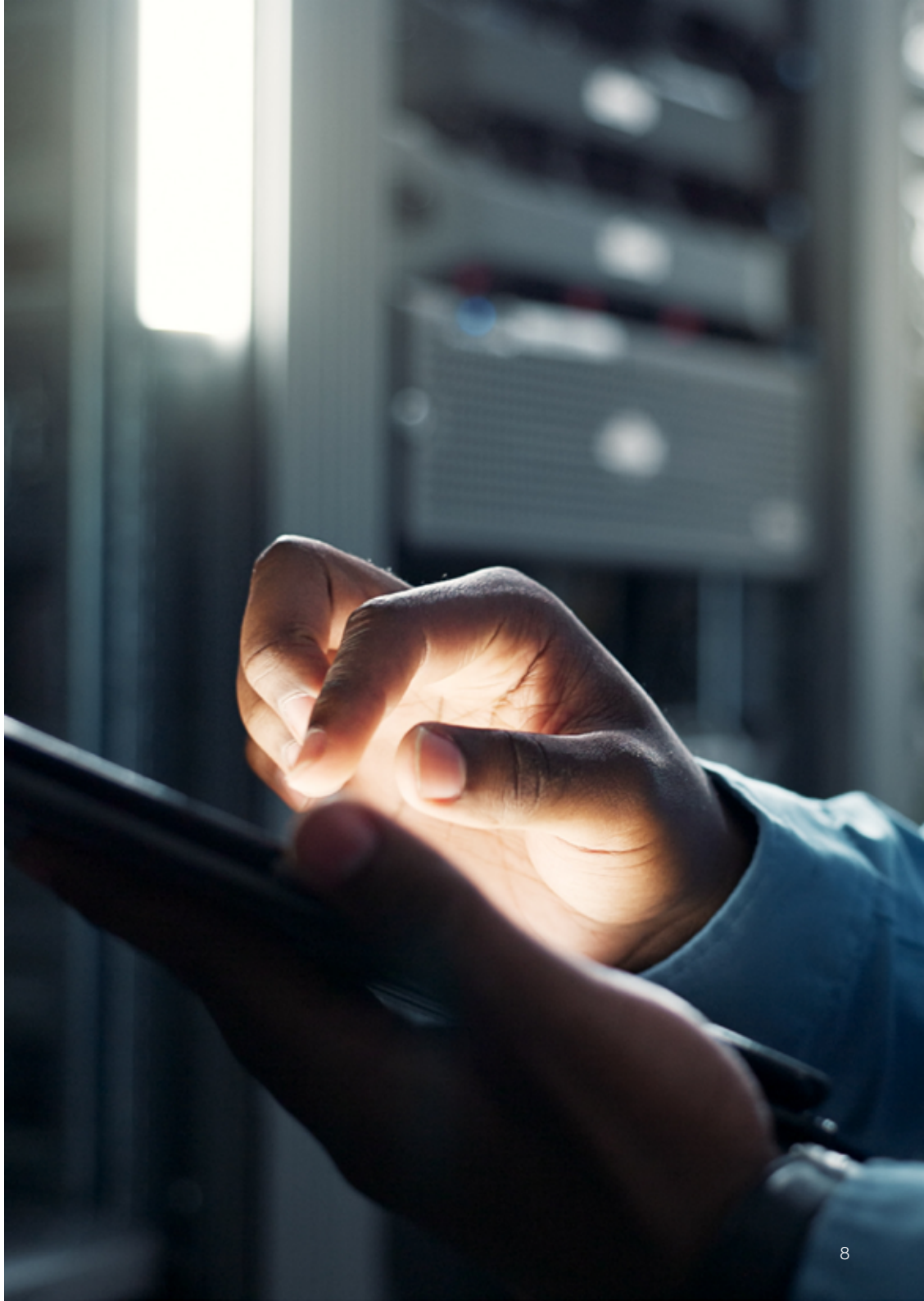
### 2.4 Aansprakelijkheid vandaag

De AI Act verdeelt toezichtstaken, maar laat het civiele aansprakelijkheidsrecht ongewijzigd. Schade door AI wordt beoordeeld zoals gebruikelijk: is er een toerekenbare tekortkoming, is een zorgplicht geschonden en bestaat er causaal verband? Een AI-systeem moet in dit verband gezien worden als een product en valt onder de vernieuwde richtlijn omtrent productaansprakelijkheid. Deze richt zich echter alleen op personen- en zaakschade. Puur financiële schade of discriminatie zijn (nog) niet benoemd.

Productaansprakelijkheid blijft leidend. Hoewel contractuele afspraken belangrijk zijn voor partijen, binden ze toezichthouders niet; buitencontractuele aansprakelijkheid blijft daardoor ongewijzigd.

## 2.5 Impact assessments

Een overheidsinstantie, een private organisatie die publieke diensten levert, een organisatie die kredietwaardigheid beoordeelt, of een instelling die risicoprofielen of prijzen voor zorg- en levensverzekeringen vaststelt, kan een hoogrisico AI-systeem in gebruik nemen. In dergelijke gevallen is er een verplichting om vóór ingebruikname de impact van het systeem op de grondrechten te toetsen. De AVG beperkt het gebruik van uitsluitend geautomatiseerde besluiten met rechtsgevolgen of significante impact op personen. Menselijk, wezenlijk toezicht is verplicht. Gebruik je AI in combinatie met persoonsgegevens, dan is een DPIA vaak noodzakelijk. Zeker in het geval van een hoogrisico AI-systeem. Deze verplichtingen blijven van kracht naast de AI Act en vereisen duidelijke governance en naleving.



# Voorbeelden en cases uit de praktijk

**1. “Overtuigend maar onjuist” – juridische bots**
Juridische Q&A-bots presteren soms verrassend goed bij eenvoudige vragen, maar missen consistentie. Ze kunnen bijvoorbeeld wetsartikelen of uitspraken ‘hallucineren’. Maak bots betrouwbaarder door het toepassingsdomein te beperken, links naar bronnen verplicht te stellen en eindresultaten altijd te laten controleren door een expert, inclusief een heldere verantwoordingsnotitie.

**2. Beeld- en audiogeneratie – fraude en bewijs**
Documenten zoals bonnetjes, schadefoto’s of rapporten kunnen door generatieve tools overtuigend worden vervalst, waardoor zelfs AI-detectors fouten maken. Procesmaatregelen zoals veilige uploads, controle van EXIF/metadata, steekproeven en alternatieve verificatie – bijvoorbeeld een koppeling met kassadata – verkleinen deze risico’s.

**3. Emotieherkenning en proctoring**
Systemen die gezichtsherkenning of emotieanalyse toepassen, zoals bij toetsbewaking, kunnen discriminerend werken en leiden tot uitsluitingen. In plaats van deze toepassingen te stoppen, is het belangrijk om kritisch na te denken over hoe ze veilig en verantwoord in HR, onderwijs of werk kunnen worden geïntegreerd. Controleer of een toepassing in een hoogrisicocategorie valt en zorg ervoor dat alle compliance vereisten volgens de AI Act op orde zijn, zodat de technologie op een veilige manier kan worden ingezet.

**4. Agents in productieomgevingen**
AI-agents die systemen zoals SharePoint of een CRM beheren, kunnen rechtstreeks invloed hebben op kritieke processen. Governance is cruciaal: werk met least privilege-toegang, sandboxing, rate limiting en logging. Stel voor de klantcommunicatie duidelijke limieten aan het uitgaand verkeer om fouten te beperken.

**5. HR en selectie**

Een generiek AI-model is geen selectie-algoritme. Wanneer je als bedrijf een generieke AI inzet voor cv-screening, kun je worden beschouwd als een aanbieder van een hoogrisico-systeem, inclusief CE-verplichtingen. Het is essentieel dat er duidelijk beleid wordt opgesteld, inclusief training in AI-geletterdheid, om verrassingen te voorkomen. Bij het gebruik van AI-systemen is het belangrijk dat de technische documentatie voldoende duidelijkheid biedt over de toepassing en de bijbehorende risico's. Het contractueel uitsluiten van hoogrisico doeleinden of het zorgen voor compliance tijdens de ontwikkeling van het systeem is van cruciaal belang.

**6. Deskilling in operationele processen**

Als AI te veel wordt vertrouwd, verslapt vaak de kritische blik. Vermijd deze 'vinkjesreflex' door actieve onderbouwing verplicht te stellen. Laat medewerkers bronnen, checks en onzekerheden documenteren en stuur op kwaliteit in plaats van doorloopsnelheid.



# Hoe Hiscox beschermt, met de juridische rugdekking van ICTRecht

**4.1 Wat verzekerbaar is en wat niet**
Aansprakelijkheid en verzekeringen in een AI-context:
In een technologiegedreven omgeving brengt zakelijke aansprakelijkheid specifieke uitdagingen met zich mee, zeker met de toenemende inzet van AI. Begrijp hoe verschillende verzekeringsoplossingen bescherming kunnen bieden.

- *Beroepsaansprakelijkheid*
  Deze verzekering beschermt tegen schadeclaims van opdrachtgevers en derden bij vermogensschade door fouten in je bedrijfsactiviteiten. In sommige gevallen vallen ook zaak- en personenschade onder de dekking.

  Gebruik je AI-technologie in je bedrijf? Denk aan AI-agenten of generatieve AI voor interne processen, als hulpmiddel bij dienstverlening, of geïntegreerd in je aanbod. Schadeclaims van derden die voortvloeien uit dit AI-gebruik zijn automatisch meeverzekerd. Daarnaast is de juridische verdediging tegen dergelijke claims inbegrepen.

  Ook als AI slechts een onderdeel vormt van je dienstverlening, kan het fouten veroorzaken. Denk aan onnauwkeurige output, systeemstoringen, contractbreuk, misleidende verklaringen, inbreuk op intellectueel eigendom, reputatieschade of privacyschendingen.

**Bij technologiebedrijven reiken de risico's verder**
Zij integreren AI-oplossingen van derden, personaliseren deze, of ontwikkelen en commercialiseren eigen AI-technologie als kernonderdeel van hun aanbod.
Dit vraagt om aanvullende verzekeringsvoorwaarden: specifieke AI-clausules, acceptatie-eisen rond logging en training, en uitgebreide contractuele afspraken met opdrachtgevers.
Technologiebedrijven met aantoonbare volwassenheid in AI-risicobeheer en bepaald doelgebruik kunnen in aanmerking komen voor verzekeringsacceptatie.

- *Cyberverzekering*
  AI kan het digitale aanvalsoppervlak vergroten, bijvoorbeeld via kwetsbare API's of kwetsbaarheden als prompt injection. Een cyberverzekering biedt hierin een vangnet, met dekking voor datalekken, systeeminbraken, forensisch onderzoek, crisiscommunicatie en herstel.

- *Bestuurdersaansprakelijkheid*
  Zonder duidelijke AI-governance riskeren bestuurders aansprakelijkheid. Nalatigheid, zoals het ontbreken van beleid, training of toezicht, valt steeds vaker onder zorgplicht.

**4.2 Underwriting: vragen die ertoe doen**

Bij AI gaat het om meer dan technologie; juiste risicobeheersing is essentieel. Hiscox beoordeelt risico's op basis van belangrijke kernthema's, zoals:

- *Gebruiksscenario*:
  Is het een laag, hoog of verboden risico volgens AI-Act?
  En is het toepassingsgebied helder? Gebruik van generatieve AI voor content of besluitvorming vraagt extra aandacht.
- *Rol verzekerde*:
  Ben je een aanbieder of alleen een gebruiksverantwoordelijke?
- *Menselijk toezicht*:
  Hoe wordt blind vertrouwen op de uitkomsten van AI voorkomen?
  En hoe wordt menselijk toezicht geborgd?
- *Data & herkomst*:
  Zijn de datasets betrouwbaar, licenties in orde en de privacy gewaarborgd?
- *Documentatie*:
  Is het doel begrensd en zijn de beperkingen duidelijk?
- *Transparantie*:
  Denk aan labeling, disclosure en beleid rond bijvoorbeeld deepfakes.
- *Logging & audit*:
  Worden modelbeslissingen en interacties vastgelegd?
- *Security*:
  Van API-beveiliging tot mitigaties tegen prompt injection.

Het zijn onder meer deze thema's die de premie en dekking bepalen. Ze bieden een duidelijke roadmap voor verzekerbaarheid. Neem voor meer informatie en advies contact op met je verzekeringsadviseur.

**4.3 Contractuele ruggengraat (met ICTRecht)**

*Contracten als sleutel tot AI-compliancy en verzekerbaarheid*

Wanneer er met AI-technologieën wordt gewerkt, is een sterke contractuele basis essentieel om zowel juridische risico's als verzekerbaarheid te waarborgen. Hierbij is aansluiting op de AI Act essentieel. Veel van de compliance vereisten die gelden, kennen een wederzijdse afhankelijkheid. Zo moet de gebruiksverantwoordelijke een adequaat niveau van menselijk toezicht toepassen. Dan moet de aanbieder het systeem dusdanig ontwerpen dat wezenlijke menselijke

tussenkomst ook mogelijk is. Anderzijds moet voorkomen worden dat partijen de gehele AI Act in een contract proberen te vatten.

Hier zijn enkele belangrijke aandachtspunten bij het opstellen van contracten:

*Rol- en scopebepaling*
Je bent aanbieder wanneer je een AI-systeem onder eigen naam op de markt brengt, ook als een extern model de kern vormt. Leg het beoogde doel en het gebruikscontext schriftelijk vast. Is sprake van een hoogrisico-AI-systeem — zoals gedefinieerd in de Europese AI Act, bijvoorbeeld omdat het systeem wordt ingezet in gereguleerde domeinen of beslissingen met juridische of wezenlijke impact op personen ondersteunt — dan gelden aanvullende verplichtingen. Maak in dat geval expliciete afspraken over verantwoordelijkheden, wederzijdse afhankelijkheden, toezicht en risicobeheersing, conform de eisen uit de AI Act.

*Gebruikshandleiding en beperkingen*
Lever een duidelijke handleiding met daarin het gebruiksdoel, technische grenzen, performance, datasetbeschrijving en mogelijke biases. Vermeld expliciet wanneer menselijk toezicht noodzakelijk is: eenvoudige toepassingen zoals spamfilters vereisen doorgaans geen toezicht, terwijl AI-tools die invloed hebben op beslissingen dit wél nodig hebben. Leg vast dat afnemers de instructies strikt naleven. Dit vermindert het risico op misbruik en fouten.

*Aansprakelijkheid en vrijwaring*
Beperk de aansprakelijkheid tot schade die ontstaat ondanks correct gebruik van het AI-systeem, conform de overeengekomen instructies en binnen de contractueel vastgelegde scope. Benadruk transparant dat toezichthouders civielrechtelijke aansprakelijkheid anders kunnen interpreteren; regel de verdeling eerlijk en bescherm jezelf contractueel. Legt vast dat de gebruikers te allen tijde zelf verantwoordelijk zijn voor de toepassing van het AI-systeem. Onduidelijke instructies binnen de scope van de toepassing kunnen alsnog tot fouten leiden.

*Transparantie en labeling*
Communiceer het AI-gebruik aan je eindgebruikers. Label deepfakes zichtbaar en gebruik technische watermerken in generatieve outputs. Deze voorzieningen worden in de praktijk vooral door grote modelleveranciers (zoals OpenAI, Google en Anthropic) ingebouwd, maar maak duidelijk dat je deze transparantievoorzieningen toepast waar ze beschikbaar zijn.

*Logging en audit*
Eis dat systemen gebeurtenissen loggen en dat afnemers logboeken bijhouden. Geef toegang tot audits, bijvoorbeeld voor modelversiebeheer en datasetwijzigingen. Bij hoogrisico-AI-systemen is het verplicht dat het systeem zelf logs bijhoudt. De gebruiker of organisatie die verantwoordelijk is voor het gebruik, moet deze logs bovendien zorgvuldig bewaren.

*Security en continuïteit*
Stel minimale securityvereisten zoals API-authenticatie, isolatie en back-ups. Borg daarnaast met voorzieningen zoals roll-back, fail-safes en kill-switches dat jouw AI veilig en betrouwbaar blijft opereren.

*Training en AI-geletterdheid*
Voorzie afnemers van verplichte onboarding, trainingsmodules en updates bij wetswijzigingen of modelaanpassingen.

Met deze aanpak ontstaat er een stevige basis voor AI-compliance én verzekerbaarheid.

**4.4 Governance en operations – het werkend krijgen**
ICTRecht en Hiscox werken samen om AI-risico's beheersbaar en verzekerbaar te maken. ICTRecht levert:

- Een AI-beleid en classificatiekader met beslisbomen en voorbeelden (laag, hoog, verboden).
- Rol- en verantwoordelijkheidsverdeling (RACI) voor aanbieders en gebruikers.
- Procesondersteuning voor de volledige model lifecycle.
- Checklists en protocollen voor menselijk toezicht.
- Transparantie- en labelingbeleid, inclusief deepfake-labels en botdisclosure.
- Specifieke incidentrespons voor AI-risico's zoals model drift en prompt injection.
- Evidence & audit: robuuste logging en dossieropbouw.

# Praktische handvatten voor AI-governance en verzekerbaarheid

Wanneer AI wordt ingezet, zijn duidelijke kaders en checklists onmisbaar. Ze helpen om risico's te beheersen en verzekerbaarheid aantoonbaar te maken.

### *A. AI-governance quickscan*

Begin met een heldere analyse:

- *Use-case*: Wat is het doel, de impact en wie zijn betrokken?
- *Classificatie*: Valt het gebruik onder laag, hoog of verboden risico's? Zijn sectorregels van toepassing?
- *Rol*: Ben je aanbieder onder eigen merk of alleen gebruiker/integrator?
- *Data*: Is de herkomst, representativiteit, rechten en bias geborgd? Wordt er met gevoelige data gewerkt?
- *Menselijk toezicht*: Wie houdt toezicht, op welke manier en wanneer?
- *Transparantie*: Welke disclosure- en labelvereisten (bijvoorbeeld watermerken) zijn van toepassing?
- *Beveiliging*: Denk aan toegangsrechten, API-beperkingen en ketenbeveiliging.
- *Logging/audit*: Welke gebeurtenissen worden vastgelegd, hoe lang en wie heeft toegang?
- *Contracten*: Hoe worden doelen, verantwoordelijkheden, aansprakelijkheid en trainingsverplichtingen afgebakend?
- *Verzekerbaarheid*: Match met beroepsaansprakelijkheid, cyber- en bestuurdersaansprakelijkheidsverzekeringen; zijn aanvullende voorwaarden nodig?

### *B. Vragen voor de verzekeringsadviseur*

Een verzekeringsadviseur kan specifieke vragen stellen, zoals:

- Welke AI-functionaliteiten levert het bedrijf en welke impact hebben ze?
- Hoe wordt biascontrole, menselijk toezicht en transparantie ingericht?
- Zijn er log- en auditprotocollen en wordt het hoogrisicogebruik contractueel uitgesloten?

### *C. Contractbijlage: de gebruikshandleiding*

- Documenteer het doel, de niet-toegestane toepassingen, prestaties, datasets, toezichtvereisten, transparantie, logging, beveiliging en support/trainingbeleid.

### *D. Incidentrespons bij AI*

- Werk stappen uit: detectie, isolatie, analyse (via logs), herstel (bijvoorbeeld roll-back), communicatie (klanten en eventueel autoriteiten) en leren via post-mortems.

# Waar ICTRecht het verschil maakt

ICTRecht vertaalt complexe wet- en regelgeving, zoals de AI Act en AVG, naar praktische tools om bedrijven direct te ondersteunen. ICTRecht biedt:

- *Contractarchitectuur*:
  Waterdichte afbakening van rollen en scope, met heldere aansprakelijkheidskaders.

- *Compliance-by-design*:
  Geïntegreerde oplossingen voor classificatie, labeling, logging en audittrails.

- *Training*:
  Praktische programma's voor productteams, sales en management.

- *Verzekerbaarheid*:
  De beschikbaarheid van documentatie en controleprocessen die nodig zijn voor verzekeringsacceptatie.

ICTRecht maakt van complexe regels een werkbare zekerheid.




HISCOX

# Conclusie
# Van experiment naar volwassen AI

AI biedt ongekende mogelijkheden voor innovatie en concurrentiekracht. Het cruciale verschil wordt gemaakt door goed georganiseerde processen en heldere kaders:

- Begrens het doel en bepaal de rol (aanbieder of gebruiker).
- Waarborg menselijk toezicht en maak beslissingen uitlegbaar.
- Organiseer contracten en procedures rond doelbinding, logging, transparantie en beveiliging.
- Toon volwassen governance om verzekerbaarheid te verbeteren.

Hiscox × ICTRecht zorgen voor begeleiding van beleid en contractvorming tot polis en audit. Zo blijven bedrijven flexibel, compliant en verzekerd, hoe hoog de lat ook ligt.



# Verklarende woordenlijst

***AI Act***
Europese verordening die AI-systemen reguleert op basis van risico's, met specifieke verplichtingen voor aanbieders en gebruikers.

***AI-agents***
Autonome of semi-autonome AI-systemen die zelfstandig taken uitvoeren, systemen aansturen of acties ondernemen op basis van doelen en context.

***Aanbieder (provider)***
Partij die een AI-systeem onder eigen naam op de markt brengt, ook wanneer gebruik wordt gemaakt van een model van een derde partij.

***API (Application Programming Interface)***
Technische koppelingslaag waarmee softwaresystemen, waaronder AI-modellen, gegevens en functionaliteiten met elkaar kunnen uitwisselen.

***Auditability (auditbaarheid)***
De mate waarin beslissingen, processen en outputs van een AI-systeem achteraf controleerbaar en reconstrueerbaar zijn.

***CE-markering (AI-context)***
Aanduiding dat een hoogrisico-AI-systeem voldoet aan de eisen van de AI Act en rechtmatig in de EU mag worden ingezet.

***Conformiteitsbeoordeling***
Formele toetsing waarmee wordt vastgesteld of een AI-systeem voldoet aan wettelijke vereisten vóór marktintroductie.

***DPIA (Data Protection Impact Assessment)***
Privacy-impactanalyse onder de AVG om risico's voor betrokkenen te beoordelen bij verwerkingen met een hoog privacyrisico, waaronder bepaalde AI-toepassingen.

***Fail-safe***
Ontwerpprincipe waarbij een systeem bij fouten of incidenten automatisch overschakelt naar een veilige toestand.

***Generatieve AI***
AI-systemen die nieuwe content genereren, zoals tekst, beeld, audio of video, op basis van patronen uit trainingsdata.

***Gebruiksverantwoordelijke***
Organisatie die een AI-systeem toepast binnen haar processen en verantwoordelijk is voor correct gebruik, toezicht en naleving.

***Hoogrisico-AI-systeem***
AI-toepassing die volgens de AI Act extra verplichtingen kent vanwege potentiële impact op veiligheid, grondrechten of rechtspositie van personen.

***Kill-switch***
Mechanisme waarmee een AI-systeem of functionaliteit direct en gecontroleerd kan worden uitgeschakeld bij ernstige risico's of misbruik.

***Least privilege-toegang***
Beveiligingsprincipe waarbij gebruikers of systemen alleen toegang krijgen tot functies en data die strikt noodzakelijk zijn.

***Menselijk toezicht (human oversight)***
Maatregelen waarmee mensen AI-uitkomsten kunnen controleren, bijsturen of ingrijpen wanneer nodig.

***Mitigaties***
Technische, organisatorische of contractuele maatregelen om geïdentificeerde AI-risico's te beperken.

***Model governance / data governance***
Beleid en processen rond herkomst, gebruik, monitoring en wijziging van AI-modellen en datasets.

***Prompt injections***
Manipulatietechniek waarbij kwaadaardige input een AI-model aanzet tot ongewenst of onveilig gedrag.

***Rate limiting***
Technische maatregel die het aantal verzoeken of acties per tijdseenheid beperkt om misbruik of overbelasting te voorkomen.

***Roll-back***
Mogelijkheid om een AI-systeem of modelversie terug te zetten naar een eerdere, stabiele toestand na fouten of incidenten.

***Sandboxing***
Het uitvoeren van systemen in een afgeschermde omgeving om schade bij fouten of misbruik te beperken.

***Synthetische teksten***
Teksten die geheel of gedeeltelijk door AI zijn gegenereerd en niet rechtstreeks door een mens zijn geschreven.

***Transparantieplicht***
Wettelijke verplichting om duidelijk te maken dat interactie of content door AI wordt gegenereerd.

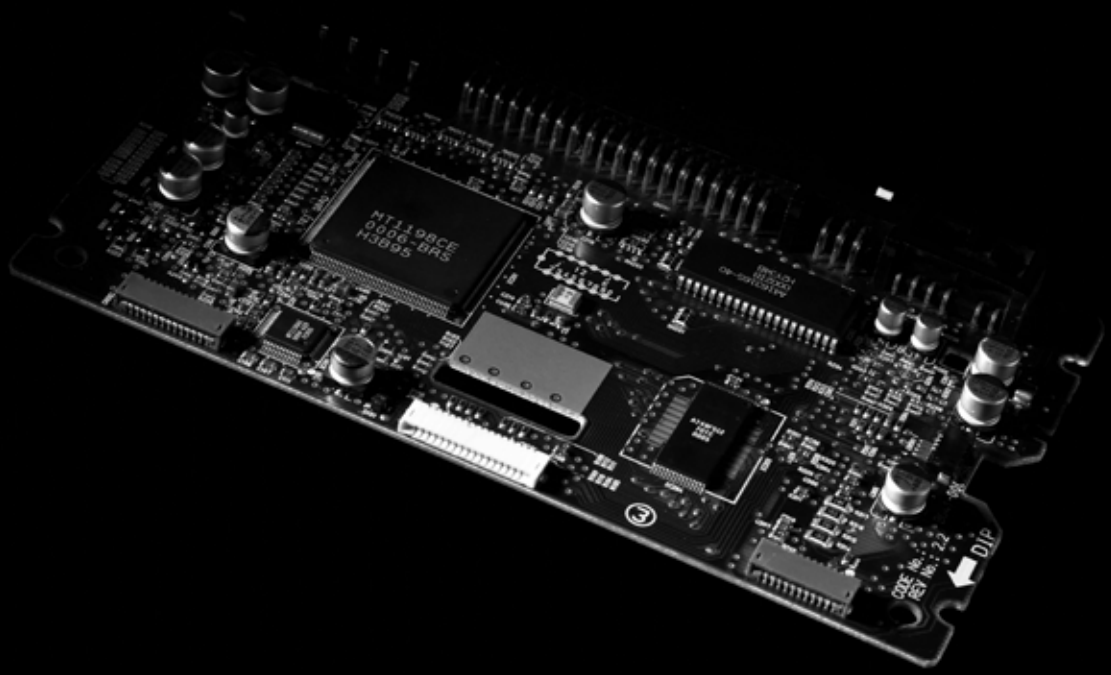
De inhoud van deze woordenlijst is afkomstig uit openbare bronnen, er kunnen geen rechten aan worden ontleend.

Hiscox Nederland
Arent Janszoon Ernststraat 595B
Postbus 87033
1080 JA Amsterdam

T 00 31 (0)20 517 0700
E hiscox.underwriting@hiscox.nl
www.hiscox.nl

ICTRecht
Jollemanhof 12
1019 GW AMSTERDAM

T 00 31 (0)20 663 1941
E contact@ictrecht.nl
www.ictrechtnl




Bezoek onze website en ontdek hoe wij je bedrijf kunnen ondersteunen.
www.hiscox.nl