

Van de Velde

Beleid rond AI



Dit beleid werd goedgekeurd door de Raad van Bestuur van Van de Velde NV op 22 april 2026.

Aan onze medewerkers

Dit beleid biedt een duidelijk kader voor het verantwoord, transparant en wettelijk gebruik van AI systemen binnen Van de Velde.



Van de Velde heeft de ambitie om het gebruik van AI te stimuleren met het oog op innovatie. We zien op korte termijn mogelijkheden op het vlak van :

- Commerciële groei via verschillende initiatieven richting de consument;
- Hogere kwaliteit en/of efficiëntie in diverse businessprocessen.

In het kader van dit beleid (hierna “Beleid”) wordt met “wij”, “we”, “ons”, “onze” of “Van de Velde” bedoeld Van de Velde NV met adres Lageweg 4, 9260 Schellebelle, België en alle directe of indirecte dochterondernemingen.

Het Management Team is verantwoordelijk voor de toepassing van het Beleid. Jaarlijks wordt het Beleid door het Management Team besproken en geëvalueerd, onder meer op volgende punten:

- EIA-resultaten (Ethical Impact Assessment)
- Effectiviteit van fairness-controles
- Incidentregistratie
- Duurzaamheid van AI-toepassingen
- Effectiviteit van menselijk toezicht

Waar nodig worden er, na goedkeuring door de Raad van Bestuur, bijsturingen en verbeteringen aangebracht aan het Beleid.

Dit Beleid biedt een duidelijk kader voor het verantwoord, transparant en wettelijk gebruik, de ontwikkeling en inzet van AI systemen binnen Van de Velde, in overeenstemming met Verordening (EU) 2024/1689 (hierna ‘AI Act’), Verordening (EU) 2016/679 (hierna ‘GDPR’) en [de waarden van Van de Velde](#).

Lees het Beleid, denk erover na, praat erover met je collega’s en vraag bij twijfel om advies. **Maar het allerbelangrijkste: hanteer de principes hieronder vermeld in je dagelijkse werk.**

Op die manier versterken we samen elkaar en het bedrijf.

Karel Verlinde*, CEO en Yvan Jansen**, voorzitter Raad van Bestuur

* als vertegenwoordiger van Karel Verlinde CommV

** als vertegenwoordiger van YJC BV

Wat verwachten we van jou?



Het Beleid geldt voor **alle medewerkers die verbonden zijn aan Van de Velde en AI systemen ontwerpen, ontwikkelen, aankopen of gebruiken in het kader van hun rol binnen Van de Velde**. Dit is met inbegrip van, maar niet beperkt tot leden Management Team, werknemers (van onbepaalde of bepaalde duur of tijdelijk), consultants, stagiairs, jobstudenten, gedetacheerd personeel, thuiswerkers, deeltijdse en uitzendkrachten, vrijwilligers en agenten.

Voor bepaalde van deze medewerkers ontbreekt een gezagsverhouding met Van de Velde (zoals het geval is bij consultants en agenten). Hier geldt:

- Het Beleid is de leidraad voor integer handelen, maar enkel contractuele afspraken zijn afdwingbaar;
- Verwijzingen naar 'leidinggevende' worden indien relevant vervangen door 'opdrachtgever' of 'contactpersoon'.

1. Respecteer het Beleid

Stel geen handelingen die kunnen leiden tot een inbreuk, of een vermoeden van inbreuk, op het Beleid.

Een medewerker die de regels schendt, dient te beseffen dat Van de Velde dit ernstig neemt. Dit kan leiden tot verschillende sancties: van een waarschuwing tot ontslag wegens ernstig wangedrag, zelfs wanneer de medewerker al lange tijd bij Van de Velde actief is en een goede staat van dienst heeft.

Bij een strafbaar feit kan de politie ingelicht worden.

2. Voltooi de training

Indien je een uitnodiging ontvangt, voltooi dan onze training rond werken met AI.

3. Geef je collega's feedback

Integriteit is veel meer dan alleen een *mooi woord of een loze belofte*. Integriteit heeft betrekking op alle medewerkers, altijd. Iedereen dient in dit verband verantwoordelijkheid op te nemen.

Van de Velde verwacht van alle medewerkers dat ze zich op het werk onberispelijk gedragen en we elkaar erop wijzen wanneer dit niet het geval is. De meeste problemen kunnen op deze wijze worden opgelost.

Bedankt alvast om deze ethische manier van werken verder mee uit te dragen.

4. Meld verdachte situaties

Indien je vermoedt dat de regels in het Beleid worden geschonden, dat er onethisch of onregelmatig AI gebruik is, en het probleem niet opgelost geraakt, verwachten we van je dat je **actie onderneemt**. Dit kan je anoniem doen.

Als je denkt dat iets niet goed zit, vragen we je dit altijd te melden. Laat je niet in een situatie dwingen waar je dingen moet doen waarvan je weet of vermoedt dat ze fout zijn.

Als je twijfels hebt, kan je in volledig vertrouwen te rade gaan bij je leidinggevende, je Management Team lid of het hoofd van het Legal Departement.

Principes van verantwoorde AI

Principes van verantwoorde AI dienen ervoor te zorgen dat AI-systemen betrouwbaar, eerlijk en veilig zijn.



1. Definities

- **AI systeem:** Een op machines gebaseerd systeem dat met wisselende autonomie functioneert, adaptiviteit toont en uit invoer output genereert die fysieke of virtuele omgevingen beïnvloedt (Artikel 3(1) van de AI Act).
- **AI systeem met een hoog risico:** Een AI systeem dat ingrijpende gevolgen kan hebben voor de gezondheid, veiligheid of grondrechten van burgers (Hoofdstuk III van de AI Act).
- **Aanbieder (provider):** Een entiteit die een AI systeem of model ontwikkelt (of laat ontwikkelen) en dit op de markt brengt of in gebruik neemt onder zijn eigen naam of merk.
- **Implementeerder (deployer):** Een entiteit of persoon die een AI systeem onder zijn eigen toezicht en verantwoordelijkheid gebruikt in het kader van een professionele activiteit.

2. Principes

A. Menselijk toezicht

AI blijft onder betekenisvolle menselijke controle. Output wordt altijd gecontroleerd door bevoegde medewerkers.

B. Eerlijkheid en non-discriminatie

Van de Velde detecteert en voorkomt stereotypering, bias en discriminerende effecten. We voeren regelmatige controles uit en bij twijfel wordt het Legal Departement geconsulteerd.

C. Veiligheid en robuustheid

AI wordt veilig gebruikt en periodiek getest.

D. Transparantie en uitlegbaarheid

Indien wettelijk vereist worden gebruikers, klanten en partners geïnformeerd wanneer zij omgaan met AI.

E. Privacy en gegevensbescherming

De verwerking van persoonsgegevens met behulp van AI systemen valt onder het toepassingsgebied van de interne privacy werkgroep ('privacy champions') van Van de Velde. In het kader van deze werkgroep worden onder meer jaarlijkse interne audits en Data Protection Impact Assessments uitgevoerd teneinde te verzekeren dat verwerkingen conform de GDPR zijn.

F. Verantwoordelijkheid

Rollen voor ontwerp, uitrol en monitoring worden duidelijk toegewezen, zowel intern als extern.

G. Ecologische voetafdruk

We gebruiken AI enkel als deze échte meerwaarde biedt.

H. Proportionaliteit en do-no-harm

AI wordt enkel ingezet wanneer deze noodzakelijk, geschikt en proportioneel is. Toepassingen die bijvoorbeeld leiden tot sociale scoring, massasurveillance of niet-omkeerbare impact worden uitgesloten.

I. Inclusiviteit en diversiteit

AI-systemen worden ontworpen, getest en beoordeeld met aandacht voor diverse gebruikersgroepen, inclusief kwetsbare of ondervertegenwoordigde groepen.

AI risicobeheer en shadow AI

A. AI-risicobeheer

Alle AI-systemen worden geklasseerd volgens de risicocategorieën van de AI Act.

Van de Velde gebruikt momenteel geen hoog risico of verboden systemen.

Voor alle significante AI toepassingen voert Van de Velde een **Ethical Impact Assessment (EIA)** uit, met aandacht voor:

- risico's voor mensenrechten, privacy en non-discriminatie
- impact op kwetsbare groepen
- proportionaliteit en alternatieven
- duurzaamheid en milieu-effecten
- stakeholderconsultatie
- mitigerende maatregelen en documentatie tijdens de volledige levenscyclus

Voor kritieke systemen wordt continue monitoring toegepast met vooraf gedefinieerde escalatie- en stopzettingcriteria.

B. Gebruik van niet-geautoriseerde AI (Shadow AI)

Om de veiligheid van bedrijfsgegevens en de naleving van de AI Act te waarborgen, hanteert Van de Velde een strikt beleid rond het gebruik van externe AI-toepassingen.

- **Geautoriseerde Tools:** Medewerkers mogen uitsluitend gebruikmaken van AI-systemen die expliciet zijn goedgekeurd door de IT-afdeling en zijn opgenomen in de interne "Approved AI List" (**Bijlage 1**).
- **Verbod op Shadow AI:** Het eigenhandig afsluiten van abonnementen of het gebruik van persoonlijke accounts voor zakelijke doeleinden op publieke AI-platforms (zoals bv. gratis versies van ChatGPT, Midjourney of Claude) is niet toegestaan voor het verwerken van niet-publieke bedrijfsinformatie.
- **Data Leakage:** Het is strikt verboden om niet-publieke bedrijfsinformatie (zoals vertrouwelijke informatie, bedrijfsgeheimen, ongepubliceerde ontwerpen of persoonsgegevens) in te voeren in niet-geautoriseerde publieke AI-modellen, aangezien deze gegevens gebruikt kunnen worden voor het trainen van externe modellen.
- **Aanvraagprocedure:** Indien een medewerker een nieuwe AI-tool wenst te gebruiken die nog niet op de goedgekeurde lijst staat, moet hiervoor een aanvraag worden ingediend bij de IT/Legal-afdeling voor een voorafgaande veiligheids- en impactbeoordeling via een Jira IT Support ticket (onder 'request new or additional access to a service or application').

Transparantie, data governance en derdenbeheer

A. Transparantie en communicatie

Gebruikers worden indien wettelijk vereist geïnformeerd wanneer AI wordt gebruikt en welke rol menselijke controle speelt.

Voor AI in klantgerichte toepassingen wordt toegankelijke informatie gepubliceerd over werking, beperkingen en rechten van betrokkenen.

B. Data governance: AVG & privacy-by-design

Gegevens in AI-systemen worden minimalistisch, rechtmatig en proportioneel verwerkt. Privacyenhancing technieken (pseudonimisering, dataminimalisatie, toegangslimieten) zijn standaard.

Bij het gebruik van AI-systemen waarbij persoonsgegevens worden verwerkt, wordt het Legal Departement in een vroeg stadium betrokken om toe te zien op de naleving van privacyrechten en het uitvoeren van de nodige effectbeoordelingen.

C. Datakwaliteit & fairness

Datasets worden geëvalueerd op:

- representativiteit
- herkomst en legitimiteit
- bias-risico's
- mogelijkheid tot inferentie van gevoelige gegevens

D. Duurzame data architectuur

Van de Velde stimuleert energie-efficiënte dataoplossingen en beperkt onnodige opslag of modeltraining.

E. Vertrouwelijkheid van invoer

Bij het gebruik van goedgekeurde generatieve AI-systemen moeten medewerkers nagaan of de "training mode" is uitgeschakeld, zodat ingevoerde bedrijfsdata niet wordt gebruikt voor de verdere ontwikkeling van het model door de provider.

F. Leveranciers- en derdenbeheer

Externe AI-systemen moeten voldoen aan:

- internationale normen rond transparantie, fairness en privacy;
- toetsing op datasetkwaliteit en modelbias;
- verplichtingen rond auditeerbaarheid, uitlegbaarheid en incidentrapportage.

Contracten met AI-aanbieders bevatten bepalingen rond:

- auditrechten;
- mitigatie- en stopzettingcriteria;
- rapportage van modelupdates, incidenten en risico's.

G. Opleiding en bewustmaking

Alle relevante medewerkers volgen verplichte AI-ethiek- en compliance opleidingen, inclusief:

- impact van AI op mensenrechten, privacy en non-discriminatie;
- bewust gebruik van AI-systemen;
- risico's van antropomorfisering ("AI lijkt iets te willen").

Teams die AI ontwikkelen of integreren volgen gespecialiseerde trainingen rond EIA, datakwaliteit, fairness en technisch ethisch ontwerp.

Een verdachte situatie melden

Meld je bezorgdheid over iedere schending of vermoeden van schending van het Beleid zo snel mogelijk. Van de Velde vertrouwt erop dat jij je verantwoordelijkheid neemt.



1. Meld bij je leidinggevende of Management Team lid

Een (vermoeden van) schending of misbruik van het Beleid meld je bij je leidinggevende of Management Team lid.

Jouw leidinggevende of Management Team lid meldt is verplicht dit te melden aan de CEO. De CEO zoekt dan zorgvuldig uit of een onderzoek vereist is. Elk onderzoek wordt op objectieve en vertrouwelijke wijze uitgevoerd op korte termijn na de melding. Indien geen onderzoek wordt ingesteld, wordt de melder van de (vermoedelijke) schending geïnformeerd, indien mogelijk met aanvullende informatie.

2. Meld via Klokkenluiderskanaal



Daarnaast kan je ook een melding doen volgens de procedure uiteengezet in het schema “Interne melding” in het **Klokkenluidersbeleid** van Van de Velde als je denkt of vermoedt dat er een conflict met het Beleid heeft plaatsgevonden, of kan plaatsvinden in de toekomst.

Onder het Klokkenluidersbeleid van Van de Velde wordt de melding vertrouwelijk behandeld en geniet de melder bescherming tegen mogelijke represailles. Bovendien kan de melding anoniem gemaakt worden. Voor vragen kan je terecht bij whistleblowing@vandevelde.eu.

Het **Klokkenluidersbeleid** is via People verkrijgbaar, via Conversation Room (Files – All – Legal Policies) en www.vandevelde.eu (Van de Velde – Klokkenluiden).



3. Vragen?

Als je niet zeker bent of een bepaalde handeling een schending van het Beleid uitmaakt, of als je andere vragen hebt, kan je dit bespreken met je leidinggevende of het hoofd van het Legal Departement via legal@vandevelde.eu of +32 9 365 25 10.

Bescherming tegen represailles

Van de Velde wil openheid aanmoedigen en zal iedereen steunen die een probleem te goeder trouw meldt, ook als er achteraf geen probleem blijkt te zijn.



Personen die onder druk worden gezet door anderen om het Beleid te overtreden, of die een probleem of misbruik door anderen melden, maken zich misschien zorgen over voor hen mogelijke negatieve gevolgen. Het kan hierbij gaan om ontslag, disciplinaire maatregelen, bedreigingen of een andere nadelige behandeling.

Als je denkt dat je het slachtoffer bent van een negatieve behandeling, kan je hiervan melding doen volgens de procedure uiteengezet in het schema “Interne melding” in het **Klokkenluidersbeleid** van Van de Velde. Je kan je hierbij beroepen op de beschermingsmaatregelen opgenomen in het Klokkenluidersbeleid.

Van de Velde hanteert een absoluut **verbod op represailles** in het kader van het Beleid.

Van de Velde stelt alles in het werk om ervoor te zorgen dat je geen negatieve behandeling hoeft te vrezen als je:

- weigert deel te nemen aan overtredingen van het Beleid;
- een melding te goeder trouw doet van een vermoeden dat een werkelijke of mogelijke overtreding heeft plaatsgevonden, of kan plaatsvinden in de toekomst.

Bijlage I

AI	Bestaande IT software	Domein	Optimalisatie door AI voor:
AI-enhanced	Microsoft 365	Company wide	Daily operations for company wide employees
AI-native	Microsoft Copilot Chat	Company wide	Daily operations for company wide employees
AI-enhanced	Contentful	Ecommerce	Content translation
AI-enhanced	SurferSEO	Ecommerce	SEO text generation / translation
AI-enhanced	Algolia	Ecommerce	Product recommendations, Synonym suggestion, MCP available
AI-enhanced	BrightCove	Ecommerce	Video captions,... currently not used
AI-enhanced	Capcut	Marketing	Video generation for social media
AI-enhanced	Canva	Marketing/Commerce	Asset & video manipulation for different channels
AI-enhanced	krea.ai	Marketing	Asset generation for different channels
AI-enhanced	kling.ai	Marketing	Video asset generation
AI-enhanced	Dalton AI	Ecommerce	AI based campaign / content optimization
AI-enhanced	Elevenlabs	Marketing	Voice AI: update language spoken on video content
AI-enhanced	JIRA	IT	Rovo
AI-enhanced	Confluence	IT	Rovo
AI-enhanced	Figma	Ecommerce	Prompt design suggestions/Transform design to code
AI-enhanced	Adobe	Marketing	Editing assets
AI-enhanced	HeyGen	Training	Training videos (translations + avatar)
AI-enhanced	WSGN	Brands&Design / marketing	Generating custom trend overview incl. ideas
AI-enhanced	DeSL	Brands&Design	PLM tool, including image creation
AI-enhanced	Insider	Digital commerce	Translations directly into the marketing automation platform
AI-enhanced	Workato	IT	MCP platform, Agent Creation, A2A communicatie Bijv. Consumer Insights Hub
AI-enhanced	Browserstack	IT	Automated website testing
AI-enhanced	Sentry	IT	Website debugging
AI-enhanced	Typeform	Ecommerce	Website forms: generate / translate
AI-enhanced	Adobe	Marketing	Asset generation / bulk operations
AI-enhanced	Microsoft Copilot Studio	IT	Create, customise and launch Ai agents
AI-enhanced	Microsoft Dynamics	Customer Service / Sales	Ai agent embedded in application
AI-enhanced	HiBob	People	Ai agent embedded in application
AI-enhanced	Databricks Data Intelligence	Data	Data Agent
AI-native	Microsoft Purview	IT	Governance en Security tool for Ai