

Van de Velde

AI policy



This policy was approved by the Board of Directors of Van de Velde NV on 22 April 2026.

To our people

This Policy provides a clear framework for the responsible, transparent and legal use of AI systems at Van de Velde.



It is Van de Velde's ambition to use AI to stimulate innovation. We see short-term opportunities in terms of:

- Commercial growth through various consumer-oriented initiatives;
- Higher quality and/or greater efficiency in various business processes.

In this policy (hereinafter referred to as the "**Policy**"), "**we**", "**our**" and "**Van de Velde**" means Van de Velde NV with address Lageweg 4, 9260 Schellebelle, Belgium and all direct and indirect subsidiaries.

The Management Team is responsible for applying the Policy. The Policy is discussed and assessed by the Management Team on an annual basis. The points covered include:

- Ethical impact assessment (EIA) results
- Effectiveness of fairness controls
- Incident registration
- Sustainability of AI applications
- Effectiveness of human supervision

Adaptations and improvements are made to the Policy where necessary, subject to approval by the Board of Directors.

This Policy provides a clear framework for the responsible, transparent and legal use, development and deployment of AI systems at Van de Velde in accordance with Regulation (EU) 2024/1689 (hereinafter the "**AI Act**"), Regulation (EU) 2016/679 (hereinafter "**GDPR**") and [the Van de Velde values](#).

Read the Policy, reflect on it, discuss it with your colleagues and ask for advice if you are unsure about anything. **But most important of all: follow the principles stated below in your day-to-day work.**

In doing so, we will make each other and the company stronger.

Karel Verlinde*, CEO, and Yvan Jansen**, Chairman of the Board of Directors

* as representative of Karel Verlinde CommV

** as representative of YJC BV

What do we expect from you?



The Policy applies to **all people who have a relationship with Van de Velde and who design, develop, buy or use AI systems in their role at Van de Velde**. This includes but is not limited to members of the Management Team, employees (on fixed-term, open-ended or temporary contracts), consultants, trainees, job students, seconded staff, people working from home, part-time and temporary agency staff, volunteers and agents.

Some of these people (such as consultants and agents) are not controlled by Van de Velde. The following applies:

- The Policy is the guide to acting with integrity but only contractual agreements are enforceable;
- Where appropriate, references to “*manager*” are replaced by “*client*” or “*contact person*”.

1. Comply with the Policy

Do not act in any way that could lead to a breach or a suspicion of a breach of the Policy.

Employees who break the rules need to understand that Van de Velde takes this seriously. Various sanctions are available, from a warning to dismissal due to serious misconduct, even for employees who have worked for Van de Velde for a long time and have a clean record.

The police may be called in to deal with a punishable offence.

2. Complete the training

If you receive an invitation, complete our Working with AI training.

3. Give your colleagues feedback

Integrity is much more than just a *buzzword* or *blah-blah*. Integrity relates to employees, at all times. Everyone must assume responsibility in this area.

Van de Velde expects irreproachable behaviour in the work setting from all employees and we call each other out if this standard is not met. Most problems can be dealt with like this.

Thank you for promoting this ethical way of working.

4. Report suspicious situations

If you suspect that the rules set out in the Policy are being broken, that AI is being used in an unethical or improper way, or that the problem is not being resolved, we expect you to **take action**. You can do so anonymously.

We ask you to always report anything you feel is not quite right. Don't allow yourself to be forced into a situation of having to do things you know or suspect to be wrong.

If you are unsure, you can approach your manager, your Management Team member or the head of the Legal Department for advice in complete confidence.

Principles of responsible AI

Principles of responsible AI serve to ensure that AI systems are reliable, fair and safe.



1. Definitions

- **AI system:** A machine-based system that operates with varying levels of autonomy, that may exhibit adaptiveness, and that infers, from the input it receives, outputs that can influence physical or virtual environments (Article 3(1) of the AI Act).
- **High-risk AI system:** An AI system that can have far-reaching consequences for the health, safety or basic human rights of citizens (Chapter III of the AI Act).
- **Provider:** An entity that develops (or commissions the development of) an AI system or model and places it on the market or puts it into service under its own name or trademark.
- **Deployer:** A natural or legal person that uses an AI system under its authority in the course of a professional activity.

2. Principles

A. Human supervision

Humans must always have meaningful control of AI. Output is always checked by authorised employees.

B. Fairness and non-discrimination

Van de Velde detects and prevents stereotyping, bias and discriminatory impacts. We run regular checks and the Legal Department is consulted if any suspicions are raised.

C. Security and robustness

AI is used securely and tested periodically.

D. Transparency and explainability

Where legally required, users, customers and partners are notified when they are interacting with AI.

E. Privacy and data protection

The processing of personal data using AI systems falls within the scope of the internal privacy workgroup (“privacy champions”) of Van de Velde. This workgroup conducts annual internal audits and data protection impact assessments are conducted to ensure processing is GDPR-compliant.

F. Responsibility

Design, rollout and monitoring roles are clearly assigned, both in-house and externally.

G. Ecological footprint

We only use AI when it adds real value.

H. Proportionality and do no harm

AI should only be used when this is deemed necessary and expedient, and when the benefits outweigh the risks. Applications that facilitate social scoring, mass surveillance or irreversible outcomes, for example, are not permitted.

I. Inclusion and diversity

AI systems are designed, tested and assessed with due consideration for various user groups, including vulnerable and underrepresented groups.

AI risk management and Shadow AI

A. AI risk management

All AI systems are classified in accordance with the risk categories in the AI Act.

Van de Velde does not currently use any high-risk or prohibited systems.

All significant AI applications are subject to an **ethical impact assessment (EIA)** by Van de Velde. Focus areas are:

- Human rights, privacy and non-discrimination risks
- Impact on vulnerable groups
- Proportionality and alternatives
- Sustainability and environmental impacts
- Stakeholder consultation
- Mitigating measures and documentation during the whole lifecycle

Critical systems are monitored continuously, for which escalation and stop criteria have been defined.

B. Use of unauthorised AI (Shadow AI)

Van de Velde has a strict policy on the use of external AI applications to ensure corporate data are protected and the AI Act is complied with.

- **Authorised tools:** People must only use AI systems that have been explicitly approved by the IT department and added to the internal “Approved AI List” (**Appendix 1**).
- **Shadow AI ban:** Personally subscribing to public AI platforms (such as free versions of ChatGPT, Midjourney or Claude) or using personal accounts for business purposes to process company information that is not in the public domain is not permitted.
- **Data leakage:** Providing company information that is not in the public domain (such as confidential information, business secrets, unpublished designs and personal data) to unauthorised public AI models is not permitted, as this data can be used to train external models.
- **Request procedure:** If an employee wishes to use a new AI tool that has not yet been placed on the Approved AI List, a Jira Support ticket must be submitted to the IT/Legal department so that a security and impact assessment can be conducted (“Request new or additional access to a service or application”).

Transparency, data governance and third-party management

A. Transparency and communication

Where legally required, users are notified when AI is used and what role human control has in the process.

Accessible information is published on operation, restrictions and rights of data subjects for AI in customer-oriented applications.

B. Data governance: GDPR and privacy by design

Data must be processed in AI systems in a minimal, lawful and proportional way. Privacy-enhancing techniques (pseudonymisation, data minimisation, access restrictions) must be used as standard.

When processing personal data using AI systems the Legal Department is involved at an early stage to ensure privacy rights are respected and the requisite impact assessments are conducted.

C. Data quality and fairness

Datasets are assessed as to:

- Representativity
- Origin and legitimacy
- Bias risks
- Possibility of sensitive data being inferred

D. Sustainable data architecture

Van de Velde encourages energy-efficient data solutions and limits unnecessary storage and model training.

E. Input confidentiality

To ensure company data is not used to develop the provider's model, people must verify that training mode is deactivated when using approved generative AI systems.

F. Suppliers and third-party management

External AI systems must comply with:

- International transparency, fairness and privacy standards;
- Dataset quality and model bias testing requirements;
- Auditability, explainability and incident reporting obligations.

Contracts with AI providers contain stipulations concerning:

- Audit rights;
- Mitigation and termination criteria;
- Model update, incident and risk reporting.

G. Training and awareness

All relevant people follow mandatory AI ethics and compliance training, including:

- Impact of AI on human rights, privacy and non-discrimination;
- Informed use of AI systems;
- Anthropomorphism risks ("The AI seems to want something").

Teams that develop or incorporate AI follow specialised EIA, data quality, fairness and ethical design training.

Report a suspicious situation

Report concerns about any breaches or suspected breaches of the Policy as soon as possible. Van de Velde expects you to act responsibly.



1. Report to your manager or a member of the Management Team

Report (suspected) violations or abuses of the Policy to your manager or a member of the Management Team.

Your manager or a member of the Management Team has an obligation to report this to the CEO. The CEO will then conduct a thorough examination to determine whether an investigation is required. All investigations are conducted in an objective and confidential way within a short timeframe. If no investigation is initiated, the person who reports the (suspected) breach will be notified and given additional information where possible.

2. File a report in the Whistleblower channel

You can also file a report using the procedure set out in the “Internal report” chart in the Van de Velde **Whistleblowing Policy** if you believe or suspect the Policy has been breached or could be breached in the future.

The report will be handled in confidence and the reporter will be protected from any reprisals in accordance with the Van de Velde Whistleblowing Policy. Reports can also be filed anonymously. Any questions can be emailed to whistleblowing@vandevelde.eu.

The **Whistleblowing Policy** can be accessed through People, in Conversation Room (Files – All – Legal Policies) and at www.vandevelde.eu (Van de Velde – Whistleblowing) .

3. Questions?

If you are unsure whether a given act constitutes a violation of the Policy or you have any other question, you can discuss this with your manager or the head of the Legal Department by emailing legal@vandevelde.eu or calling +32 9 365 25 10.

Protection from reprisals

Van de Velde wants to encourage openness and will support anyone who reports an issue in good faith, even if this ultimately proves to be unfounded.



Persons who are pressurised by others to breach the Policy or who report an issue or abuse by others may be concerned about possible negative consequences for themselves. These could take the form of dismissal, disciplinary measures, threats or detrimental treatment.

Van de Velde imposes a total **ban on reprisals** under the Policy.

Van de Velde does its utmost to ensure that you need not fear negative consequences if you:

- Refuse to take part in breaches of the Policy;
- File a report in good faith that you suspect a breach has occurred or could occur in the future.

You can also file a report using the procedure set out in the “Internal report” chart in the Van de Velde **Whistleblowing Policy** if you believe or suspect the Policy has been breached or could be breached in the future. In doing so, you can rely on the protective measures set out in the Whistleblowing Policy.

Appendix I

AI	Existing IT software	Domain	AI enhanced for:
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 optimalization
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