

Van de Velde

Politique relative à l'IA



Cette politique a été approuvée par le Conseil d'administration de Van de Velde SA le 22 avril 2026.

À tous nos collaborateurs

Cette politique fournit un cadre clair pour l'utilisation responsable, transparente et légale des systèmes d'IA au sein de Van de Velde.



Van de Velde ambitionne de stimuler l'utilisation de l'IA en vue de favoriser l'innovation. À court terme, nous distinguons des opportunités sur le plan de :

- La croissance commerciale au travers de différentes initiatives visant les consommateurs ;
- L'amélioration de la qualité et/ou efficacité de divers processus de l'entreprise.

Dans le contexte de la présente politique (ci-après dénommée « **Politique** »), « **nous** », « **notre** » ou « **Van de Velde** » désignent Van de Velde NV, dont l'adresse est Lageweg 4, 9260 Schellebelle, Belgique, et toutes ses filiales directes ou indirectes.

La Management Team est responsable de l'application de la Politique. Celle-ci est discutée et évaluée annuellement par la Management Team, plus spécifiquement sur les points suivants :

- Résultats EIA (Ethical Impact Assessment, évaluation de l'impact éthique)
- Efficacité des contrôles relatifs à l'équité
- Enregistrement des incidents
- Durabilité des applications IA
- Efficacité du contrôle humain

Le cas échéant, et après approbation du Conseil d'administration, elle est modifiée et améliorée.

Cette politique fournit un cadre clair pour l'utilisation responsable, transparente et légale, ainsi que le développement et le déploiement des systèmes d'IA au sein de Van de Velde conformément au règlement (UE) 2024/1689 (ci-après dénommé « **Loi sur l'IA** »), au règlement (UE) 2016/679 (ci-après dénommé « **RGPD** ») et aux [valeurs de Van de Velde](#).

Lisez la Politique, réfléchissez-y, discutez-en avec vos collègues et en cas de doute, posez des questions. **Mais par-dessus tout, mettez ses principes en pratique dans votre travail quotidien.**

C'est ainsi que nous nous renforcerons mutuellement et renforcerons l'entreprise.

Karel Verlinde*, CEO et Yvan Jansen**, président du Conseil d'administration

* en tant que représentant de Karel Verlinde CommV

** en tant que représentant de YJC BV

Qu'attendons-nous de vous ?



Cette Politique s'applique à **tous les collaborateurs liés à Van de Velde qui conçoivent, développent, achètent ou utilisent des systèmes d'IA dans le cadre de leur fonction au sein de Van de Velde**. Cela inclut, sans s'y limiter, les membres de la Management Team, les employés (avec contrat à durée indéterminée, déterminée ou temporaire), les consultants, les stagiaires, les étudiants jobistes, le personnel détaché, les télétravailleurs, les collaborateurs à temps partiel, les intérimaires, les bénévoles et les agents.

Pour certains de ces collaborateurs, il n'existe pas de relation d'autorité avec Van de Velde (par ex. les consultants et les agents). En ce qui les concerne :

- La Politique est le guide qui sous-tend les actions menées avec intégrité, mais seuls les accords contractuels sont applicables ;
- Les références au « *supérieur* » sont le cas échéant remplacées par « *client* » ou « *personne de contact* ».

1. Respectez la Politique

Abstenez-vous de toute activité susceptible de mener à une violation ou à une suspicion de violation de la présente Politique.

Tout collaborateur qui viole les règles doit savoir que Van de Velde prend la problématique très au sérieux. Toute violation peut mener à diverses sanctions, allant du simple avertissement au renvoi pour faute grave, même si le collaborateur travaille pour l'entreprise depuis longtemps et y a de bons états de service.

En cas d'infraction pénale, la police peut être prévenue.

2. Menez à bien la formation

Si vous recevez une invitation, menez à bien notre formation relative au travail avec l'IA.

3. Donnez du feedback à vos collègues

L'intégrité est bien plus qu'un joli mot ou une fausse promesse. Elle concerne tous les collaborateurs, à tout moment. Chacun a sa part de responsabilité.

Van de Velde attend de tous ses collaborateurs qu'ils se comportent de façon irréprochable au travail et qu'ils se mettent mutuellement face à leurs responsabilités lorsque ce n'est pas le cas. C'est généralement de cette façon que l'on parvient à résoudre la plupart des problèmes.

Merci d'avance pour votre implication continue dans cette manière de travailler éthique.

4. Signalez les situations suspectes

Si vous suspectez une violation des règles de la Politique ou une utilisation contraire à l'éthique ou induite de l'IA et que le problème n'est pas résolu, nous attendons de vous que vous **preniez des mesures**. Cela peut se faire anonymement.

Nous vous demandons de toujours signaler toute action suspecte. Ne vous laissez pas embrigader dans des situations où vous seriez amené à faire des choses dont vous savez ou soupçonnez qu'elles ne sont pas admises.

En cas de doute, vous pouvez vous adresser en toute confiance à votre supérieur.e, au.à la membre de la Management Team qui vous représente ou au.à la responsable du département Legal.

Principes d'une IA responsable

Les principes d'une IA responsable doivent garantir que les systèmes d'IA sont fiables, équitables et sûrs.



1. Définitions

- **Système d'IA** : Un système automatisé qui est conçu pour fonctionner à différents niveaux d'autonomie, peut faire preuve d'une faculté d'adaptation et qui génère, à partir des entrées qu'il reçoit, des sorties (output) qui peuvent influencer les environnements physiques ou virtuels (Article 3 paragraphe 1 de la Loi sur l'IA).
- **Système d'IA à haut risque** : Un système d'IA susceptible de porter atteinte à la santé, à la sécurité ou aux droits fondamentaux de citoyens (Chapitre III de la Loi sur l'IA).
- **Fournisseur (provider)** : Une entité qui développe un système ou un modèle d'IA (ou le fait développer) et le met sur le marché ou en service sous son propre nom ou sa propre marque.
- **Déployeur (deployer)** : Une entité ou personne qui utilise un système d'IA sous sa propre autorité et responsabilité dans le cadre d'une activité professionnelle.

2. Principes

A. Contrôle humain

Le système d'IA reste sous un contrôle humain pertinent. Les sorties sont toujours contrôlées par des collaborateurs compétents.

B. Équité et non-discrimination

Van de Velde détecte et évite l'application de stéréotypes, les préjugés et les effets discriminatoires. Nous menons régulièrement des contrôles et le département Legal est consulté en cas de doute.

C. Sécurité et robustesse

Le système d'IA est utilisé en toute sécurité et testé régulièrement.

D. Transparence et explicabilité

Lorsque la loi l'exige, les utilisateurs, les clients et les partenaires sont informés qu'ils interagissent avec un système d'IA.

E. Respect de la vie privée et protection des données

Le traitement de données personnelles par des systèmes d'IA entre dans le champ d'application du groupe de travail interne sur le respect de la vie privée (« privacy champions ») de Van de Velde. Dans le cadre de ce groupe de travail, des audits internes annuels et des Data Protection Impact Assessments sont notamment réalisés afin de garantir que les traitements sont conformes au RGPD.

F. Responsabilité

Les rôles de conception, déploiement et monitoring sont clairement attribués, tant en interne qu'à l'extérieur.

G. Empreinte écologique

Nous n'utilisons l'IA que si elle représente une valeur ajoutée.

H. Proportionnalité et absence de préjudice

L'IA n'est utilisée que si elle est nécessaire, pertinente et proportionnelle. Les applications qui mènent, par exemple, à une notation sociale, une surveillance de masse ou un impact irréversible sont exclues.

I. Inclusivité et diversité

Les systèmes d'IA sont conçus, testés et évalués en accordant une attention particulière à divers groupes d'utilisateurs, y compris les groupes de personnes vulnérables ou sous-représentées.

Gestion du risque IA et IA fantôme (shadow AI)

A. Gestion du risque IA

Tous les systèmes d'IA sont répartis selon les catégories de risque de la Loi sur l'IA.

Actuellement, Van de Velde n'utilise ni système à haut risque ni système interdit.

Pour toutes les applications IA importantes, Van de Velde mène une **Ethical Impact Assessment (EIA)**, en prêtant une attention particulière :

- aux risques pour les droits humains, le respect de la vie privée et la non-discrimination
- à l'impact sur les groupes de personnes vulnérables
- à la proportionnalité et aux alternatives
- à la durabilité et à l'impact sur l'environnement
- à la consultation des parties prenantes
- aux mesures d'atténuation et à la documentation sur l'ensemble du cycle de vie.

Pour les systèmes critiques, une surveillance continue est assurée, avec des critères d'escalade et d'arrêt prédéfinis.

B. Utilisation d'un système d'IA non autorisé (IA fantôme)

Afin de garantir la sécurité des données de l'entreprise et le respect de la Loi sur l'IA, Van de Velde applique une politique stricte concernant l'utilisation d'applications d'IA externes.

- **Outils autorisés** : Les collaborateurs ne peuvent utiliser que des systèmes d'IA explicitement approuvés par le service informatique et figurant sur la liste interne des systèmes d'IA approuvés (Approved AI List) (**Annexe 1**).
- **Interdiction de l'IA fantôme** : La souscription personnelle d'abonnements ou l'utilisation de comptes personnels à des fins professionnelles sur des plateformes publiques d'IA (telles que les versions gratuites de ChatGPT, Midjourney ou Claude) n'est pas autorisée pour le traitement d'informations non publiques sur la société.
- **Fuite de données** : Il est strictement interdit de saisir des informations non publiques sur la société (telles que des informations confidentielles, secrets d'entreprise, projets non publiés ou données personnelles) dans des modèles d'IA publics non autorisés car ces données peuvent être utilisées pour l'apprentissage de modèles externes.
- **Procédure de demande** : Si un collaborateur souhaite utiliser un nouvel outil IA qui ne figure pas encore sur la liste approuvée, il doit introduire une demande d'évaluation préalable de la sécurité et de l'impact de cet outil auprès du département IT/Legal au moyen d'un ticket de support informatique Jira (sous « Request new or additional access to a service or application »).

Transparence, gouvernance des données et gestion des tiers

A. Transparence et communication

Si la loi l'exige, les utilisateurs sont informés lorsque l'IA est utilisée et sur le rôle du contrôle humain.

Concernant l'IA dans des applications orientées clients, des informations claires sur le fonctionnement, les restrictions et les droits des personnes concernées sont publiées.

B. Gouvernance des données : RGPD et privacy-by-design

Dans les systèmes d'IA, le traitement des données est réduit au strict minimum, légal et proportionnel. Les techniques de protection de la vie privée (pseudonymisation, minimisation des données, limites d'accès) sont la norme.

En cas d'utilisation de systèmes d'IA traitant des données personnelles, le département Legal est impliqué à un stade précoce pour surveiller le respect du droit à la vie privée et réaliser les analyses d'impact nécessaires.

C. Qualité des données et équité

Les ensembles de données font l'objet d'une évaluation concernant leurs :

- représentativité
- origine et légitimité
- risques liés aux préjugés
- potentiel d'inférence de données sensibles.

D. Architecture durable des données

Van de Velde encourage les solutions efficaces sur le plan énergétique du traitement des données et limite les conservations inutiles ou l'entraînement des modèles.

E. Confidentialité des entrées

Lorsqu'ils utilisent des systèmes d'IA générative approuvés, les collaborateurs doivent s'assurer que le mode entraînement (« training mode ») est désactivé afin que les données d'entreprise saisies ne soient pas exploitées pour le développement ultérieur du modèle par le fournisseur.

F. Gestion des fournisseurs et des tiers

Les systèmes d'IA externes doivent respecter :

- les normes internationales relatives à la transparence, à l'équité et au respect de la vie privée ;
- la vérification de la qualité des ensembles de données et de l'absence de biais dans les modèles ;
- les obligations relatives au caractère auditable, à l'explicabilité et au signalement des incidents.

Les contrats avec les fournisseurs d'IA intègrent des dispositions relatives :

- aux droits d'audit ;
- aux critères d'atténuation et de cessation ;
- au signalement de mises à jour de modèle, d'incidents et de risques.

G. Formation et sensibilisation

Tous les collaborateurs concernés sont dans l'obligation de suivre des formations sur l'éthique et la conformité en matière d'IA, dont :

- l'impact de l'IA sur les droits humains, le respect de la vie privée et la non-discrimination ;
- l'utilisation éclairée des systèmes d'IA ;
- les risques liés à l'anthropomorphisme (« l'IA semble vouloir quelque chose »).

Les équipes qui développent ou intègrent l'IA suivent des formations spécialisées sur l'EIA, la qualité des données, l'équité et la conception technique éthique.

Signaler une situation suspecte

Si vous vous préoccupez d'une violation ou d'une suspicion de violation de la présente Politique, signalez-le le plus rapidement possible. Van de Velde compte sur vous pour prendre vos responsabilités.



1. Signalement auprès de votre supérieur ou du membre de la Management Team qui vous représente

Toute (suspicion de) violation de la Politique doit être communiquée à votre supérieur.e ou au.à la membre de la Management Team qui vous représente.

Ces derniers sont tenus de communiquer l'information au.à la CEO. Le.la CEO jugera alors de la nécessité d'une enquête. Toute enquête éventuelle est menée de manière objective et confidentielle dans les plus brefs délais après le signalement. Si aucune enquête n'a lieu, la personne qui a communiqué la suspicion de violation en sera avertie et recevra, si possible, des informations complémentaires.

2. Signalement au moyen du canal Lanceurs d'alerte



Si vous soupçonnez l'existence ou le risque d'apparition d'un conflit par rapport à la présente Politique, vous pouvez le signaler en suivant la procédure décrite dans le diagramme « Signalement interne » de la **Politique relative aux lanceurs d'alerte** de Van de Velde.

Conformément à la Politique relative aux lanceurs d'alerte de Van de Velde, le signalement est traité de manière confidentielle et le lanceur d'alerte bénéficie d'une protection contre d'éventuelles représailles. De plus, le signalement peut être effectué de façon anonyme. En cas de question, veuillez écrire à whistleblowing@vandevelde.eu.

La **Politique relative aux lanceurs d'alerte** est disponible auprès de People, sur la Conversation Room (Files – All – Legal Policies) et sur www.vandevelde.eu (Van de Velde – Lancer une alerte interne).



3. Des questions ?

Si vous avez des incertitudes concernant le fait qu'une action donnée constitue une violation de la Politique, ou si vous avez d'autres questions, vous pouvez contacter votre supérieure.e ou le département Legal à l'adresse legal@vandevelde.eu ou au +32 9 365 25 10.

Protection contre les représailles

Van de Velde veut encourager l'ouverture et soutiendra quiconque signalera de bonne foi un problème, même s'il s'avère ultérieurement qu'il n'y a pas de problème.



Les personnes poussées par d'autres à violer la Politique ou qui signalent un problème ou un acte délictueux dans le chef de tiers s'inquiètent parfois des retombées négatives qu'elles pourraient subir. Il peut s'agir d'un licenciement, de mesures disciplinaires, de menaces ou tout autre traitement préjudiciable.

Si vous pensez être la victime d'un traitement négatif, vous pouvez le signaler en suivant la procédure décrite dans le diagramme « Signalement interne » de la **Politique relative aux lanceurs d'alerte** de Van de Velde. Vous pouvez invoquer les mesures de protection prévues dans cette Politique.

Van de Velde **interdit formellement toute forme de représailles** dans le cadre de la Politique.

Van de Velde met tout en œuvre pour que vous n'ayez à craindre aucune retombée négative si vous :

- refusez de contrevenir à la Politique ;
- signalez de bonne foi l'existence d'une violation ou d'une suspicion de violation effective, potentielle ou susceptible de se produire à l'avenir.

Annexe I

IA	Software IT existant	Domaine	Optimisé par l'IA pour:
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 communication 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