Artificial Intelligence Policy

25/03/2026

Table of content

I. Introduction

Vermeg is committed to the ethical, transparent, and secure use of Artificial Intelligence (AI) tools in its operations. As an organization certified under ISO/IEC 27001:2022 and ISO/IEC 27701:2019, Vermeg ensures that AI technologies are used responsibly and in alignment with international standards, particularly ISO/IEC 42001:2023 (AI Management System).

This policy provides a governance framework for the responsible use of AI within Vermeg. It ensures that AI tools support efficiency, innovation, and quality without compromising security, privacy, or compliance obligations.

This policy aligns with:

- ISO/IEC 42001:2023 : Artificial Intelligence Management System
- ISO/IEC 27001:2022 : Information Security Management System
- ISO/IEC 27701:2019 : Privacy Information Management System
- EU AI Act (2024) principles on trustworthy and responsible AI use

A. Scope and Applicability

This policy applies to the use of AI technologies across Vermeg. It covers:

-
- Internal productivity tools (e.g., coding assistants, document generation tools) used by employees to support daily tasks.
- AI components embedded in Vermeg products or services, which may rely on external AI providers.
- AI tools used for operational decision support, assisting employees in analysis, drafting, or problem-solving activities..
- All departments, subsidiaries, and entities of Vermeg.
- All data processed, entered, and/or generated by AI tools.

B. Objectives

The objectives of this policy are to:

1. Ensure the ethical and secure use of AI tools within Vermeg.
2. Protect the confidentiality, integrity, and privacy of all information processed through AI.
3. Ensure compliance with legal, contractual, and regulatory obligations.
4. Prevent misuse of AI systems and manage associated risks.
5. Promote awareness and accountability among all AI tool users.

II. Governance and Responsibilities

Vermeg maintains a centralized governance model for AI usage oversight under the Information Security team.

Roles and Responsibilities

Role	Responsibilities
Executive Management	Approves the AI Usage Policy and ensures alignment with corporate strategy.
AI team	Manage AI tools.
Information Security team	Gouvernance & oversees responsible AI usage, risk management, and compliance with ISO 42001 , 27001, 27701 standards.
IT teams	Manage deployment, licensing, and access to approved AI tools.

Data Protection Officer (DPO)	Ensures AI usage complies with data protection and privacy regulations.
Leagl team	Ensures AI use respects IP rights, and legal requirements; Validates AI vendor contracts.
Employees &Contractors	Use AI responsibly, protect data confidentiality, and comply with all internal guidelines.

III. Responsible Use Principles

Vermeg's approach to AI usage is based on the following principles:

1. Transparency : Clearly understand and disclose when AI tools are being used.
2. Human Oversight :Ensure AI assists, but does not replace, human decision-making:

    - AI-generated outputs must always be reviewed and validated by a human before being used in deliverables, code, documentation, or communications.
    - Users remain fully responsible for the accuracy, legality, and compliance of any content produced with AI assistance.
    - AI-generated content should not be considered authoritative without verification, particularly for technical, legal, financial, or client-facing materials.

3. Privacy and Security : Never input or share confidential, sensitive, or client data with public AI tools.
4. Accountability : Each user is accountable for ensuring responsible and compliant AI usage.
5. Fairness and Accuracy : Validate AI outputs before using them in any business context.
6. Compliance: Use only tools and licenses approved by Vermeg.

IV. AI Tools Authorization, Access and Acquisition:

Vermeg authorizes the use of AI systems strictly limited to those officially licensed and approved by the company for business purposes. The deployment or utilization of any public or unapproved AI tools outside approved systems is not permitted under any circumstances.

Access to AI tools is managed in accordance with Vermeg's established access management policy ; as defined in VER_ISO_PR_001_EN Information Security Procedures.

Permissions are granted based on job roles and justified business needs to ensure that AI systems are used appropriately and securely**.**The IT and Security teams regularly monitor the access to AI tools.

Prior to the adoption or use of any Artificial Intelligence (AI) tool, Vermeg shall conduct a comprehensive assessment to evaluate the provider's capabilities, data protection practices, and security measures. The assessment aims to identify potential gaps, including those related to data privacy, data handling, intellectual property, and access controls, based on the criteria defined in Appendix A - AI Provider Compliance Checklist. If significant gaps are identified, the AI tool shall not be approved for use.Approved AI providers may be subject to periodic reassessment to ensure continued compliance with Vermeg's security, privacy, and contractual requirements.

V. Data Protection and Security

A. Data Handling Rules

Vermeg employees and contractors must not enter any sensitive, personal, or client-related information into public AI tools. Only approved and secure systems may be used when handling company data.

All information used in AI-assisted tasks must be accurate, authorized, and processed in accordance with Vermeg's internal standards.

Vermeg employess and contractors are responsible for verifying that the data they use complies with the company's security and confidentiality requirements.

All data processed by AI tools must follow Vermeg's VER_ISO_PR_001_EN Information Security Procedures to ensure full compliance with internal and regulatory obligations.

B. Storage and Retention

AI tools used within Vermeg must not store confidential information, complying with a Zero Data Retention Policy, ensuring that input data is not used for model training, in alignment with Vermeg's **VER_ISO_PR_005_EN Records Retention Schedule**.

C. Privacy Compliance

All AI usage within Vermeg must comply with applicable privacy regulations, including ISO 27701, and Vermeg's internal privacy framework.

VI. Prohibited Practices

The following are strictly prohibited within Vermeg:

- Using unlicensed or public AI tools for company tasks.
- Using AI to create false, biased, or harmful content: Ensure AI-generated materials align with Vermeg values and policies.
- Using AI for automated decision-making that impacts individuals without review.
- Using AI tools for personal projects - Company time and resources -

Violations may result in disciplinary actions per Vermeg's HR Procedures.

VII. Awareness and Training

AI training and awareness are integrated into Vermeg's overall Information Security Awareness Program. All employees and contractors are required to participate in these training activities and adhere to the established guidelines

VIII. Risk Management:

The management of AI-related risks follows Vermeg's established Risk Management Methodology, as defined in VER_ISO_PR_006_EN Vermeg Risk Management Methodology. This ensures that all potential impacts associated with the use of Artificial Intelligence are identified, assessed, and treated in accordance with Vermeg's risk management framework.

IX. Incident Management

Employees and contractors must promptly report any potential AI-related incidents or events in accordance with Vermeg's Incident Management Procedure, as defined in VER_ISO_PR_001_EN Information Security Procedures.

Any irregular or inappropriate behavior by AI must be reported immediately (AI-related incidents are considered security incidents).

X. Communication & transparency

Communication regarding AI usage is managed in alignment with Vermeg's Communication Plan, as outlined in VER_ISO_PO_004_EN Vermeg IMS Manual.

This ensures that both internal and external communications related to AI are consistent, accurate, and compliant with Vermeg's IMS.

Vermeg is committed to maintaining transparency in the use of Artificial Intelligence. Impacted parties are informed, where appropriate, about the purpose and outcomes of AI usage systems that may affect them. All approved AI tools are recorded in Vermeg's Application Risk Register to ensure visibility, accountability, and traceability of AI usage across the organization.

XI. Review and Continuous Improvement

This policy shall be reviewed annually or upon major changes.

Lessons from audits, incidents, and new technologies will drive ongoing improvements.

XII. Definitions

Term	Definition
AI Tool	Any software or system using artificial intelligence to assist in tasks.
Authorized AI Tool	AI service officially licensed and approved by Vermeg for professional use.
Public AI Tool	Any AI platform freely available on the internet without a corporate license & data control.
Responsible Use	Using AI ethically, securely, and in line with Vermeg's data and compliance policies.
AI Decision Impacting Individuals	Any AI-generated output or automated decision that could affect a person's rights, opportunities,or treatment. Such decisions require appropriate human review.

XIII. Appendix A - AI Provider Compliance Checklist

(For internal reference: vendor evaluation, authorization checklist for AI tool approval.)