Docply — AI Act Compliance Suite

F03-02

AI Governance Policy

Top-level AI policy approved by senior management

Version 1.0

Issued on *[Insert date]*

Aligned with Regulation (EU) 2024/1689 (EU AI Act) and ISO/IEC 42001:2023

Document control

Document code	F03-02	**Document title**	AI Governance Policy
Version	1.0	**Date**	*[Insert date]*
Document owner	*[CEO / Senior management sponsor]*	**Approved by**	*[Board / CEO]*
Classification	Internal	**Status**	*[Draft / Approved / Issued]*

Revision history

Version	Date	Author	Description of changes
1.0	*[Date]*	*[Author]*	Initial issue
[v]	*[Date]*	*[Author]*	*[Describe changes]*

Approval

Role	Name	Signature	Date
Prepared by — Document owner	*[Name]*		*[Date]*
Reviewed by — AI Compliance Officer	*[Name]*		*[Date]*
Approved by — Senior management	*[Name]*		*[Date]*

1. Policy statement

[Insert company name] ("the Organisation") is committed to the responsible development, provision and use of Artificial Intelligence (AI) systems. This Policy establishes the framework that governs how the Organisation:

- Complies with Regulation (EU) 2024/1689 (the EU AI Act) for any AI system it develops, places on the market, puts into service, imports, distributes or uses in the European Union.
- Operates an Artificial Intelligence Management System (AIMS) aligned with ISO/IEC 42001:2023, intended to enable continual improvement of AI governance and, where applicable, third-party certification.
- Manages AI-related risks to the health, safety, fundamental rights and legitimate interests of natural persons, the environment, and the Organisation itself.
- Promotes a culture of trustworthy AI, characterised by lawfulness, ethical alignment, robustness, transparency, accountability, fairness and respect for human autonomy.

This Policy is approved by senior management and applies to all personnel, contractors and third parties acting on behalf of the Organisation in connection with AI systems.

2. Scope

2.1 Organisational scope

This Policy applies to *[Insert legal entity / entities, business units, geographies covered]*. Subsidiaries, branches and joint ventures within the scope are listed in *[Insert reference, e.g. annex or organisational chart]*.

2.2 Material scope

This Policy covers all AI systems that the Organisation:

- **Develops** — internally or by commissioning third parties — and places on the market or puts into service under its own name or trademark (provider role).
- **Uses** in a professional capacity (deployer role).
- **Imports** from third countries into the Union (importer role).
- **Distributes** on the Union market (distributor role).

It also covers general-purpose AI (GPAI) models where the Organisation acts as their provider.

2.3 Exclusions

This Policy does not apply to AI used in the course of personal, non-professional activity, nor to AI systems explicitly excluded from the scope of the AI Act (e.g. systems exclusively for military, defence or national security purposes, where applicable).

3. Guiding principles

The Organisation adopts the following principles, which are reflected in all procedures and templates of the Compliance Set:

3.1 Lawfulness and rights protection

AI systems are designed, developed and used in compliance with applicable law, including the AI Act, the GDPR, sector-specific regulation, and fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union.

3.2 Risk-based approach

The Organisation manages AI on a risk-based approach. Resources, controls and oversight are calibrated to the level of risk posed by each AI system, with stricter controls for high-risk AI systems and prohibited practices excluded from the AI portfolio.

3.3 Human oversight

The Organisation ensures that AI systems can be effectively overseen by natural persons during their period of use, with measures proportionate to the risk, level of autonomy and context of use.

3.4 Transparency

Users, deployers and affected persons are informed of the use of AI systems where required, and provided with sufficient information about capabilities, limitations and intended purpose to enable informed use and review.

3.5 Fairness and non-discrimination

Datasets used to train, validate and test AI systems are managed to be relevant, sufficiently representative, and — to the best extent possible — free of errors and bias. Outputs are monitored to detect and mitigate adverse impacts on individuals or groups.

3.6 Robustness, accuracy and security

AI systems are designed and developed to achieve appropriate levels of accuracy, robustness and cybersecurity, and to perform consistently throughout their lifecycle.

3.7 Accountability

Clear roles and responsibilities are assigned across the AI lifecycle, including a single accountable owner for each AI system. Decisions, assumptions and trade-offs are documented to enable review.

3.8 Continual improvement

The AIMS is continually improved on the basis of monitoring, audits, incidents, lessons learned and feedback from interested parties.

4. Governance structure

The Organisation establishes the following governance structure for AI. Detailed responsibilities are set out in F03-04 RACI Matrix and in each individual procedure of the Compliance Set.

4.1 Senior management

Senior management (or the Board, where applicable) approves this Policy, sets AI-related strategic objectives, allocates resources and is ultimately accountable for compliance with the AI Act and conformity with ISO/IEC 42001.

4.2 AI Governance Committee

A cross-functional AI Governance Committee is established, chaired by the *[Insert role — e.g. Chief Compliance Officer / CIO]*. The Committee includes representatives of *[Legal, Compliance, Data Protection, Information Security, Product, Data Science / AI Engineering, Risk, HR, and business unit owners as relevant]*.

Responsibilities include:

- Approving the AI System Inventory and risk classifications
- Endorsing high-risk AI system deployments and substantial modifications
- Reviewing serious incidents and corrective actions
- Receiving the outputs of the management review (ISO/IEC 42001 Clause 9.3)

4.3 AI Compliance Officer

The AI Compliance Officer (or equivalent role designated by the Organisation) acts as the operational lead for AI compliance, owns the Compliance Set on a day-to-day basis, coordinates audits and serves as the primary point of contact with competent authorities.

4.4 AI System Owner

Each AI system has a single named AI System Owner, accountable for compliance throughout the system's lifecycle, including risk management, data governance, testing, documentation, monitoring and decommissioning.

4.5 Roles and responsibilities matrix

A complete RACI matrix covering all procedures is maintained as F03-04 RACI Matrix, which forms an integral part of this Policy.

5. The Compliance Set

The Organisation operates the following structured documentation to implement this Policy. A complete map and naming convention is provided in F03-01 Architecture document.

5.1 Foundational documents

- F03-02 AI Governance Policy (this document)
- F03-03 AI Governance Glossary
- F03-04 RACI Matrix
- F10-03 AI System Inventory

5.2 Shared procedures (AIG-PR-XX)

Thirteen shared procedures address processes covered by both the AI Act and ISO/IEC 42001, ranging from AI system classification (F05-01) and risk management (F05-02) to incident management (F09-02) and vendor management (F10-01).

5.3 AI Act-specific procedures (AIA-PR-XX)

Fourteen procedures cover obligations specific to the AI Act, including conformity assessment, deployer-specific obligations, GPAI incident reporting and limited-risk transparency.

5.4 ISO/IEC 42001-specific procedures (AIMS-PR-XX)

Nine procedures cover management-system-specific requirements such as context and scope, internal audit, management review and continual improvement.

5.5 Templates and registers

Operational templates and registers (AIG-TPL-XX, AIA-TPL-XX, AIMS-TPL-XX) support the procedures and produce the records required by both frameworks.

6. Risk management

The Organisation maintains an AI-specific risk management approach, consistent with Art. 9 of the AI Act and Clauses 6.1.2 and 6.1.3 of ISO/IEC 42001:2023, operationalised in F05-02 AI Risk Management Procedure.

AI risks are identified, analysed, evaluated and treated throughout the AI lifecycle. Residual risks are subject to formal acceptance by senior management against pre-defined risk acceptance criteria. The Organisation explicitly excludes prohibited practices defined under Article 5 of the AI Act from its AI portfolio.

7. Data governance

The Organisation manages datasets used for the development, validation and testing of AI systems in accordance with F08-01 Data Governance Procedure, addressing the requirements of Art. 10 of the AI Act and Annex A.7 of ISO/IEC 42001:2023. This includes provenance, quality, relevance, representativeness, bias evaluation, mitigation measures and where applicable lawful basis under the GDPR.

8. Human oversight, transparency and AI literacy

The Organisation ensures that high-risk AI systems are designed and used so as to allow effective human oversight (Art. 14 AI Act). Transparency obligations under Art. 13 (instructions for use) and Art. 50 (limited-risk transparency) are implemented through F11-03, F11-07 and F11-08.

All personnel involved in the development, operation and use of AI systems undergo AI literacy training appropriate to their role, in accordance with F03-05 AI Literacy, Competence and Awareness Procedure (Art. 4 AI Act; Clause 7.2-7.3 ISO/IEC 42001).

9. Supply chain and third-party AI

Third-party AI components, including general-purpose AI models, foundation models and external services, are managed through F10-01 Vendor and Third-Party AI Procedure (Art. 25 AI Act; Annex A.10 ISO/IEC 42001). Contractual clauses ensure that information and cooperation needed for compliance flow along the AI value chain.

10. Incident management and reporting

The Organisation operates an AI incident management process (F09-02) covering identification, classification, containment, investigation, root-cause analysis, corrective action and reporting. Serious incidents within the meaning of Art. 73 AI Act are reported to the relevant national competent authority within the regulatory deadlines, including the 72-hour rule applicable to providers of GPAI models with systemic risk under Art. 55.

11. Monitoring, measurement, audit and review

The Organisation monitors and measures the performance of the AIMS and of individual AI systems through:

- **F09-01 Post-Market Monitoring / Performance Evaluation Procedure (Art. 72 AI Act; Clause 9.1 ISO/IEC 42001)**
- **AIMS-PR-07 Internal Audit Procedure** (Clause 9.2 ISO/IEC 42001)
- **AIMS-PR-08 Management Review Procedure** (Clause 9.3 ISO/IEC 42001)

Outputs of monitoring, audits and reviews feed continual improvement (AIMS-PR-09) and corrective actions (F09-03).

12. Interfaces with other frameworks

This Policy is implemented in coordination with adjacent frameworks operated by the Organisation, including:

- **GDPR / Data protection — Data Protection Impact Assessments (Art. 35 GDPR) are integrated with AI System Impact Assessments (F05-03) where AI systems process personal data**
- **Information security (e.g. ISO/IEC 27001, NIS2)** — AI cybersecurity controls (Art. 15 AI Act) leverage existing information security management
- **Quality management (e.g. ISO 9001)** — Where present, the QMS is extended to cover the AI Act QMS requirements (Art. 17)
- **Sector-specific regulation** — Financial services, medical devices, automotive, energy and other sector frameworks are integrated with AI-specific obligations on a system-by-system basis

13. Communication and training

This Policy is communicated to all personnel and made available to interested parties as appropriate. Training on the Policy and the Compliance Set is delivered to relevant roles upon onboarding and at least annually thereafter.

14. Policy review and update

This Policy is reviewed at minimum annually, and on an ad-hoc basis when:

- The AI Act is amended or new EU implementing or delegated acts are issued
- ISO/IEC 42001 or supporting standards are updated
- Material changes occur in the Organisation's AI portfolio, business model or organisational structure
- Significant incidents, audit findings or external events suggest the need for revision

Updates are approved by the same authority that approved the original version.

15. Consequences of non-compliance

Failure to comply with this Policy may result in disciplinary action in accordance with the Organisation's HR policies, contractual remedies for third parties, and — where applicable — legal action. Personnel are encouraged to report concerns through F11-10 Whistleblowing Procedure for AI Issues.

16. Authority and effective date

This Policy is issued under the authority of *[Insert role and name — e.g. CEO]*. It takes effect on *[Insert effective date]* and supersedes any previous AI-related policy of the Organisation.