

AI Governance Policy for [Company Name]

Compliance with EU AI Act, GDPR, and Ethical Standards

1. Introduction

This policy establishes a structured framework to ensure ethical development, deployment, and monitoring of AI systems at [Company Name]. Aligned with the EU AI Act, GDPR, and global best practices, it prioritizes accountability, transparency, fairness, and privacy while mitigating risks.

2. Scope & Objectives

- **Scope:** Applies to all AI systems developed, procured, or used by [Company Name], including high-risk applications (e.g., hiring, healthcare, credit scoring).
 - **Objectives:**
 - Ensure compliance with EU AI Act and GDPR.
 - Mitigate ethical risks (bias, privacy breaches).
 - Foster stakeholder trust through transparency and accountability.
-

3. Governance Structure

Objective: Define roles and accountability.

- **AI Ethics Officer (AEO):**
 - Oversees policy implementation, reports to the board.
 - **AI Ethics Committee:**
 - Cross-functional team (Legal, IT, HR, external experts).
 - Reviews high-risk AI projects, conducts bias audits, approves AIAs.
 - **AI Governance Task Force:**
 - Monitors regulatory updates (e.g., EU AI Act amendments).
-

4. Risk Management & Compliance

Objective: Proactively identify and mitigate risks.

- **Risk Categorization:**
 - **Unacceptable Risk:** Prohibited systems (e.g., social scoring).
 - **High Risk:** Requires conformity assessments (e.g., hiring algorithms).
 - **Minimal Risk:** Basic transparency obligations.
 - **AI Impact Assessment (AIIA):**
 - Mandatory for high-risk systems.
 - Evaluates societal impact, bias, and compliance (template in *Appendix A*).
 - **Mitigation Strategies:**
 - Technical: Robustness testing, adversarial training.
 - Operational: Fallback protocols, incident response plans.
-

5. Transparency & Accountability

Objective: Ensure clarity in AI decision-making.

- **Algorithmic Transparency Reports:**
 - Document data sources, logic, biases (e.g., Google-style transparency reports).
 - Publicly disclose AI use cases impacting users (e.g., chatbots, recommendation engines).
 - **Accountability Framework:**
 - Assign roles: Model Developer (design), Deployer (implementation), Auditor (compliance).
 - Record decisions in an AI Audit Trail (tools: IBM OpenPages, OneTrust).
-

6. Fairness & Bias Mitigation

Objective: Eliminate discriminatory outcomes.

- **Bias Audits:**
 - Conduct quarterly using IBM AI Fairness 360 or Microsoft Fairlearn.
 - Audit results reviewed by the AI Ethics Committee.
- **Diverse Data & Teams:**
 - Ensure training data represents diverse populations.

- Involve multidisciplinary teams in model development.
-

7. Data Privacy & Security

Objective: Align with GDPR and protect user rights.

- **Privacy-by-Design:**
 - Implement techniques: differential privacy, federated learning.
 - Anonymize datasets pre-training.
 - **Data Protection Impact Assessment (DPIA):**
 - Required for AI systems processing sensitive data.
-

8. Ethical AI Design

Objective: Prioritize human rights and societal well-being.

- **Ethical Guidelines:**
 - Adopt IEEE's Ethically Aligned Design principles.
 - Prohibit AI applications conflicting with human dignity (e.g., manipulative AI).
 - **Human Oversight:**
 - Mandatory human review for high-risk decisions (e.g., loan approvals).
-

9. Stakeholder Engagement & Training

Objective: Embed a culture of ethical AI.

- **Stakeholder Workshops:**
 - Quarterly sessions with employees, customers, and regulators.
 - **Training Programs:**
 - **Employees:** Annual training on EU AI Act, GDPR, and bias mitigation.
 - **Technical Teams:** Certifications on tools like TensorFlow Privacy.
-

10. Monitoring & Continuous Improvement

Objective: Ensure ongoing compliance and adaptability.

- **Real-Time Monitoring:**
 - Tools: Fiddler AI for performance drift, Splunk for anomaly detection.
- **Annual Audits:**
 - Internal: Quarterly reviews by the AI Ethics Committee.
 - External: Third-party audits for ISO 42001 certification.
- **Feedback Mechanisms:**
 - Collect input via employee surveys, user forums, and incident reports.

Compliance Checklist for EU AI Act

Requirement	Action	Responsible Party
Prohibited AI Systems	Ban social scoring, manipulative AI	Legal Team
High-Risk Conformity Assessment	Conduct AIIA, obtain CE marking	AI Ethics Committee
Transparency Obligations	Publish algorithmic reports	Product & Compliance Teams

Implementation Roadmap

1. **Q1:** Appoint AEO, establish Ethics Committee.
 2. **Q2:** Roll out AIIA process, bias audit tools.
 3. **Q3:** Launch transparency reports, employee training.
 4. **Q4:** Conduct first external audit, publish annual review.
-

Appendices

- **Appendix A:** AI Impact Assessment (AIIA) Template
 - **Appendix B:** Algorithmic Transparency Report Example
 - **Appendix C:** Training Program Syllabus
-

References

- EU AI Act (2024)
- GDPR (2016)
- IEEE Ethically Aligned Design (2019)
- IBM AI Fairness 360 Toolkit

*Prepared by: [Kudakwashe Chimera], AI Governance Officer,
Date: [02-02-2025]*

This policy ensures [Company Name] leverages AI responsibly while building public trust and meeting regulatory obligations.