fenergo | Whitepaper

Fenergo AI Governance



© Copyright Fenergo

Table of Contents

Executive Summary	3
The Regulatory Landscape	4
Fenergo's SaaS AI Control Framework	5
Security by Design	7
Continuous Improvement & Client Empowerment	7
Leveraging AWS Bedrock for Trusted LLM Integration	8
Client Outcomes: Turning Governance into Business Value	9
Conclusion	10



Executive Summary

Trustworthy AI is essential for responsible innovation and maintaining client confidence in a rapidly changing digital world. As global standards for AI governance continue to mature, organisations must embed transparency, accountability, and ethical safeguards across their AI lifecycle. This whitepaper introduces Fenergo's SaaS AI Control Framework, which translates these principles into operational requirements. It details how the framework embeds compliance, secures data boundaries, and empowers clients to deploy Fenergo's AI capabilities with confidence.



The Regulatory Landscape

Fenergo's AI governance approach is designed to meet the needs of various major jurisdictions.

European Union
Designed to conform with the core requirements of the EU Artificial Intelligence Act, including AI system risk classification (prohibited, high, limited, minimal), conformity assessments, provider registration in the EU database for high-risk systems, post-market monitoring obligations and incident reporting obligations.

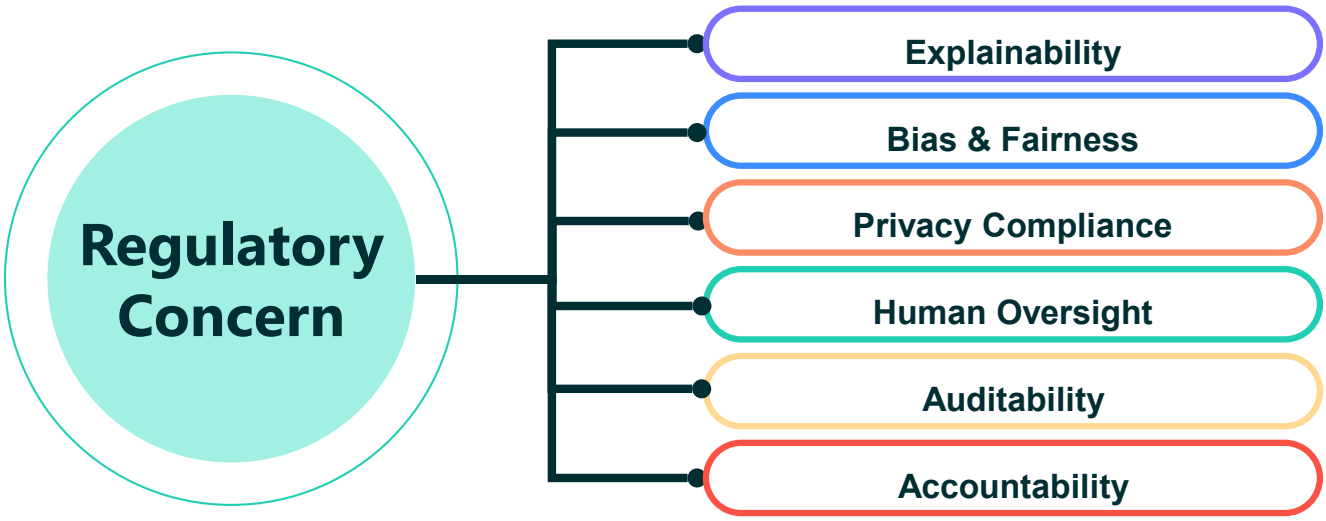
United States
Aligned with core elements of voluntary governance frameworks such as the NIST AI Risk Management Framework (AI RMF 1.0) and the Presidential Executive Orders on safe, secure, and trustworthy AI.

United Kingdom
Aligned with the UK's principles-based approach to AI regulation, which empowers existing regulators (e.g., FCA, ICO and PRA) to interpret and apply five cross-sector AI governance principles including transparency, fairness, accountability, safety, and contestability.

Singapore
Implements the FEAT (Fairness, Ethics, Accountability, and Transparency) principles issued by the Monetary Authority of Singapore (MAS) for financial institutions, alongside broader AI governance guidance under the Personal Data Protection Commission (PDPC) and Infocomm Media Development Authority (IMDA) Model AI Governance Framework.

Hong Kong
Aligned with the ethical AI guidance published by the Office of the Privacy Commissioner for Personal Data (PCPD) and the Office of the Government Chief Information Officer (OGCIO), which promote transparency, explainability, and accountability in AI design and use, consistent with the Personal Data (Privacy) Ordinance (PDPO).

Australia
Alignment with the Australian Prudential Regulation Authority (APRA) standards: CPS 230 (Operational Risk Management, Outsourcing, and Third-Party Risk) and CPS 234 (Information Security), as well as obligations under the Privacy Act 1988 relevant to AI data handling, including data minimisation, retention limitation, and security requirements.



Fenergo's SaaS AI Control Framework

Fenergo's SaaS AI Control Framework establishes over 30 distinct controls, each mapped to jurisdiction specific AI requirements and industry best practices. This includes prescriptive safeguards across the AI development lifecycle, from design and deployment to monitoring and retirement.



AI Control Framework Principles:



Explainability

Transparency is at the heart of Fenergo's AI capabilities. We've introduced an agent rationale functionality to ensure users can always understand the reasoning behind agent behaviour. These explanations are presented in a structured way, enabling users to review and assess decisions in context. This is critical not just for operational understanding but for satisfying internal audit and external regulatory requirements.



Bias & Fairness Mitigation

Fenergo applies a deliberate and systematic approach to mitigating bias and promoting fair outcomes across all AI interactions. Fenergo's AI capabilities are built on AWS Bedrock and utilize foundation mode that are not trained on client data or historical datasets, reducing the risk of introducing legacy bias. Our AI capabilities are designed to deliver consistent results regardless of the user or context, ensuring that every query is processed under the same objective conditions. Inputs are evaluated based purely on technical parameters, without any influence from user identity, role, or subjective context. This design ensures that outcomes are neutral, reliable, and in line with regulatory expectations around fairness, transparency, and responsible AI use.



Privacy Compliance

Data privacy and client confidentiality are core principles embedded throughout Fenergo's platform. Client data is not used to train or fine-tune the underlying models, and each tenant is segregated to ensure strict data isolation, with processing limited to documented purposes. All client data remains within the same geographic region as the client's AWS tenancy, supporting compliance with data sovereignty and localisation requirements.



Human Oversight

Human oversight is an essential component of the Fenergo SaaS AI control framework. Importantly, agents can be configured to perform tasks independently within predefined boundaries, but the platform is also configurable to ensure actions remain subject to review and escalation, which is vital for regulated organisations who need to demonstrate control over automated processes. The Fenergo SaaS provides full visibility into each action taken by the AI, allowing clients to drill down into every action and intervene where required. This setup ensures our AI capabilities support operational efficiency while preserving human accountability.



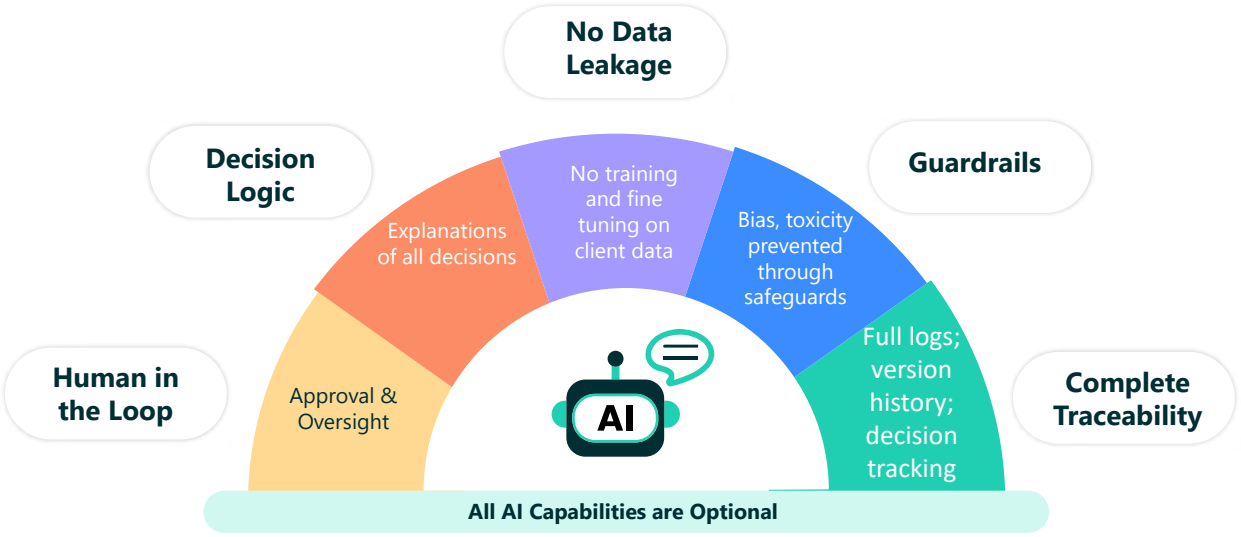
Auditability

Fenergo's platform is built to deliver full traceability with every agent action logged in a systematic and consistent way. It provides information on the agent responsible for initiating the action, the time it took place, and the conditions under which it happened. These records ensure clients can view historical activity, understand decision paths, and track the rationale behind specific outputs. This level of traceability supports both internal operational risk management and external regulatory audits. Clients can be confident that all actions are transparent, recoverable, and explainable at any point in time.



Accountability

All AI features are opt-in and/or require clients to configure how and when AI capabilities are used. Clients can oversee AI activity, adjust parameters, and override outputs as needed. The models being used are consistent across all clients, ensuring that no hidden variability is introduced. Clients are supported with the tools, documentation, and oversight mechanisms required to maintain full control. In doing so, Fenergo helps organisations meet their compliance obligations while unlocking the operational benefits of AI in a controlled and transparent way.



Security by Design

Security is foundational to Fenergo's AI capabilities. Client sensitive data is encrypted at rest and in transit using industry standard algorithms and protocols, ensuring both confidentiality and integrity. AI interactions are specifically engineered to prevent direct access by large language models to client data, maintaining strict data isolation. Access controls are rigorously enforced, with no default access to client data granted to employees or contractors. These practices are aligned with Fenergo's adherence to internationally recognized standards, including ISO/IEC 27001 and SOC 2, which validate the effectiveness of its information security and risk management frameworks. Fenergo also employs real-time monitoring tools to continuously observe system and network activity, enabling early detection of potential threats through analytics and machine learning. Security events are logged and analysed to support rapid response, with detailed reporting that informs ongoing performance improvements and strategic decision making. Furthermore, Fenergo is underpinned by robust, industry standard programs for incident response, vulnerability management, and disaster recovery, reinforcing its operational resilience and commitment to security by design.

Continuous Improvement & Client Empowerment

Fenergo's approach to AI is grounded in continuous improvement and updates are delivered through a controlled, continuous deployment model built on AWS Bedrock, with every enhancement tested and validated to ensure stability, compatibility, and performance. This means clients get the benefit of ongoing innovation without disruption, all while maintaining the transparency and control they expect. Clients can customise some AI capabilities with their own knowledge base, configuring client specific instructions and logic to suit their workflows. Separately, clients can provide feedback thorough a variety of different channels including our Early Adopter Program, Client Council or directly to their Client Partners and / or Customer Support.



Leveraging AWS Bedrock for Trusted LLM Integration

Fenergo's AI capabilities almost exclusively run through AWS Bedrock, providing a trusted foundation for secure and compliant AI deployment. This partnership ensures that models are never trained using client data, preserving data isolation, privacy, and integrity. Our close collaboration with AWS reflects a shared commitment to responsible AI innovation, reinforced by AWS's achievement of ISO/IEC 42001 certification, the international standard for AI management systems. By leveraging AWS Bedrock, Fenergo achieves consistent performance while maintaining regulatory-grade protections. This approach delivers both operational reliability and robust data protection for clients across jurisdictions.

While all agentic AI capabilities leverage AWS bedrock, where alternative technical or operational approaches are required to deliver or support other AI capabilities, these are managed under Fenergo's AI Governance processes. Each use case is formally risk-assessed and documented to ensure that it delivers an equivalent standard of control, assurance, and regulatory compliance to that established within the SaaS AI Control Framework.



Client Outcomes: Turning Governance into Business Value

Fenergo's AI governance framework is built to do more than meet compliance requirements. It is designed to deliver real, measurable value to our clients. By embedding the SaaS AI control framework at the core of our AI strategy, clients can adopt our AI capabilities with confidence.



Regulatory Alignment and Audit Readiness

Our SaaS AI Control framework enables clients to align with regulatory requirements across multiple jurisdictions. The Fenergo SaaS offers full visibility into every AI action, providing a clear view of what happened, when it occurred, and why a specific decision was made. This transparency supports both internal governance and external audit readiness.



Operational Oversight and Decision Control

Clients retain full operational control over the use of AI within their environments. Human approvals can be configured, and all AI actions are logged and can be reviewed at any time. Our shared model design ensures that the behaviour of the AI capabilities remains consistent across all clients and use cases, removing the risk of unpredictable or variable performance.



Data Protection and Privacy Assurance

From a privacy and data protection perspective, our approach is both strict and transparent. All AI processing takes place within the client's chosen AWS region, ensuring alignment with data residency and localisation requirements. Client data is never used to train or fine-tune models and is not retained beyond its intended use. Encryption, access controls, and strict processing limits ensure that client data always remains protected.



Strategic Flexibility and Client Empowerment

Clients can choose to adopt and configure AI capabilities according to their preferences. Opting in and configuring these features requires client action, and documentation, as well as configurable settings, are available on the Fenergo platform. Feedback is actively encouraged through a variety of channels, with improvements integrated into our roadmap. Our use of AWS Bedrock for foundational model services provides additional assurance around performance, security, and compliance, without introducing unnecessary complexity or exposure.



A Platform for Responsible Innovation

Fenergo's AI governance approach allows clients to embrace the benefits of AI while maintaining oversight, integrity, and compliance across their operations. It is not simply a safeguard but a strategic enabler for responsible innovation.



Conclusion

The Fenergo SaaS AI Control Framework sits at the heart of how we design, deliver, and govern our AI capabilities. It translates high level principles such as transparency, accountability, and ethical safeguards into practical operational requirements that guide every stage of the AI lifecycle. From initial design through deployment and oversight, the framework ensures our AI capabilities are not only effective but also explainable, secure, and compliant by design. As the regulatory landscape matures, Fenergo will continue to evolve the framework to stay ahead of expectations and industry standards. Responsible AI is engineered into the fabric of the Fenergo platform to help clients unlock value, build trust, and future proof their operations.



fenergo

For further information about Fenergo

Visit **www.fenergo.com**

Email us
discover@fenergo.com

About Fenergo

Fenergo is a global leader in AI-powered solutions for client lifecycle management (CLM), specializing in know your customer (KYC) and anti-money laundering (AML) compliance transformation for financial institutions.

By leveraging agentic AI and automation to bolster CLM, Fenergo empowers organizations to streamline operations, reduce costs, automate compliance processes and enhance client experience across over 120 jurisdictions. Its FinCrime Operating System, powered by Agentic AI, enables firms to supercharge efficiency gains, while maintaining governance and control in line with global AI regulations. For more information about Fenergo's market-leading AI-powered KYC/AML solutions, visit www.fenergo.com.