Fenergo AI FAQ

May 2026

© 2026 Fenergo Limited.

fenergo

Future-Proofing Client Lifecycle Management

Introduction

Fenergo's Agentic AI helps financial institutions meet their compliance objectives by automating task-based, policy-driven activities such as screening resolution, document validation, and data sourcing within the Fenergo platform. Each Agent operates under client-defined control, performing discrete compliance tasks rather than making final regulatory decisions. All actions are clearly labelled, supported by human-readable rationales, and immutable audit-logged for transparency and assurance. Clients determine where and how Agents are applied, selecting from manual, semi-autonomous, or fully autonomous modes to align with internal policies and risk appetite. This ensures automation enhances efficiency and consistency, while final decisions and accountability remain firmly with the financial institution. The following FAQ provides a deeper look at Fenergo's AI capabilities from a compliance and governance perspective, highlighting how explainability, auditability, and policy alignment are embedded into the design of every AI capability within the Fenergo platform.

Topic	Question	Response
Use of harmonised standards	What harmonised standards does Fenergo align with in the development of its AI capabilities?	Fenergo initially developed its AI Governance Framework to align with the requirements of the EU AI Act. Recognising the evolving global regulatory landscape, the framework has since been expanded to incorporate key AI laws, standards, and guidance from multiple jurisdictions. As a global provider, this approach allows Fenergo to support AI capabilities in its platform that align with international standards for compliance, security, and trust across all regions where the company operates.
AI Role	How does Fenergo determine the role and classification of its AI systems?	Fenergo's Product & Engineering function collaborates closely with the Privacy & Risk team to conduct integrated Privacy and AI Governance Impact Assessments throughout the product development processes. These assessments determine Fenergo's role in accordance with applicable regulatory frameworks.
Categorisation & Prohibited Use	How does Fenergo classify and restrict AI use?	A comprehensive Privacy & AI Governance Impact Assessment is conducted for AI capabilities to ensure a conservative, safety-focused approach from the outset. Each AI capability undergoes a detailed evaluation to determine its specific risk

©2026 Fenergo Limited. All rights reserved.

		profile and to establish the necessary governance and control requirements. Fenergo ensures ongoing alignment with applicable AI regulatory frameworks and is fully prepared to meet all associated requirements arising from these impact assessments.
Literacy	How are staff trained to handle AI related responsibilities?	Fenergo maintains a dedicated team of AI specialists responsible for the design and development of the AI capabilities within the Fenergo platform. This team collaborates closely with our Privacy and Risk function, which is formally trained in the regulatory, ethical, and operational requirements of responsible AI. In parallel, members of these teams participate in targeted AI training programs and regularly attend industry conferences and regulatory forums to stay current with emerging standards, technologies, and obligations. Together, these cross functional teams operate under an AI governance framework to ensure that all AI capabilities integrated into our SaaS platform are developed in a manner that is secure, compliant, and aligned with global best practices.
CE Marking	When does CE Marking apply?	Where an AI capability developed by Fenergo is classified by design as high risk under applicable regulatory frameworks, our Privacy & AI Governance Impact Assessments will trigger the necessary conformity assessment procedure. Where required, Fenergo will complete either internal control verification or external third-party conformity assessment, as mandated by the applicable Annex of the EU AI Act. Upon successful completion, and where necessary, a CE marking will be affixed, signifying compliance with the EU AI Act.

©2026 Fenergo Limited. All rights reserved.

Registration	When does registration apply?	Fenergo conducts rigorous Privacy and AI Governance Impact Assessments across all AI capabilities as part of its product development process. Where a high-risk AI classification is assigned, the applicable conformity assessment procedures are undertaken in line with relevant jurisdictional requirements. In the context of the EU, this will include registration in the EU AI Database in accordance with the EU AI Act. This approach ensures regulatory compliance, transparency, and accountability across all regions in which Fenergo operates.
Risk Management	How are AI risks managed?	Fenergo maintains a dedicated Risk Management team, working in close coordination with a distributed network of risk champions embedded across business units. This governance structure ensures that operational risks, including those emerging from the deployment, integration, and lifecycle management of Artificial capabilities are systematically identified, assessed, mitigated, and monitored. To address the unique risk vectors introduced by AI, such as bias and explainability, Fenergo integrates Privacy & AI impact assessments into its product development process. These assessments consider both technical and organisational controls and adhere to our AI governance framework, which is based on leading standards and regulatory expectations, including the EU AI Act, NIST AI RMF, PDPC guidance, and OGCIO & PDPC AI guidelines. The efficacy of these safeguards is subject to regular review, including client led audits and independent third-party certifications such as ISO/IEC 27001, SOC 2 Type 2 and ISO/IEC 42001.

©2026 Fenergo Limited. All rights reserved.

Impact & Conformity Assessments	What assessments are performed?	Fenergo integrates Privacy & AI Governance impact assessments into its product development process. These assessments consider both technical and organisational controls required to adhere to our Fenergo AI Governance Framework. This is based on leading standards and regulatory expectations, including the EU AI Act, NIST AI RMF, PDPC guidance, and OGCIO & PDPC AI guidelines. Where an AI capability developed by Fenergo is determined to be high risk AI following our Privacy and AI Governance Impact Assessments, it will be subject to the applicable conformity assessment procedures as mandated by relevant regulatory frameworks, and where required, the involvement of a notified body for third-party assessment. These procedures ensure the AI capability meets the applicable requirements for transparency, accountability, and human oversight.
Post-Market Monitoring	How are AI features monitored after deployment?	Fenergo ensures the ongoing efficacy of applicable AI capabilities through a structured post-market monitoring system. This includes, where applicable, the ongoing evaluation of system performance in real-world conditions, proactive identification and documentation of anomalies, malfunctions, or incidents, and the regular updating of risk assessments and technical documentation. Feedback loops with our client base are established to collect and analyse input. These activities are complemented by internal reviews, client led audits, and independent third-party assessments such as ISO 27001, ISO 27701, ISO 42001 and SOC 2 Type 2, ensuring continued conformity and safe operation throughout the AI system's lifecycle.

©2026 Fenergo Limited. All rights reserved.

External Conformity Assessment	When are external reviews needed?	Fenergo maintains a comprehensive internal governance framework designed to ensure regulatory compliance, technical robustness, and alignment with applicable standards. As such, third-party conformity assessments are generally not required. However, where a specific risk profile, client requirement, or regulatory expectation necessitates independent validation, Fenergo will engage qualified third-party assessors to supplement its internal assurance processes.
Processing Personal Data Sandbox	Can production data be processed in non-production systems?	No - Sensitive production data is not permitted in any of our SDLC tenants. Such data is only processed within designated production or "gold" tenants that are subject to appropriate security and compliance controls.
Bias and Fairness, Transparency	What is your approach to mitigating bias, and using data to train models?	Fenergo employs a structured and proactive strategy to mitigate bias across its AI capabilities, ensuring fairness, transparency, and regulatory alignment: **1. Foundation Model Integrity:** Fenergo's AI solutions are built on AWS Bedrock and utilize foundation models that undergo rigorous testing and validation by both AWS and Anthropic. These models are not trained on potentially biased historical datasets, reducing inherent bias risks from the outset. **2. Content Based Document Processing:** KYRA: Docs evaluates documents on their content, without consideration of any characteristics associated with the document owner, supporting impartiality in classification and data extraction. **3. Human Oversight:** All automated decisions are fully transparent and can be reviewed and

©2026 Fenergo Limited. All rights reserved.

		overridden by human operators, ensuring accountability and traceability. **4. Explainability:** The system provides clear, understandable reasoning behind each decision, supporting both auditability and verification requirements. **5. Impartial Query Handling:** Queries are optimized using purely technical parameters, with no influence from user identity or subjective context. **6. Consistent Outcomes:** AI generated outputs are consistent across users, irrespective of who initiates the query. **7. Equitable Access:** All authorized users have equal access to insights and data driven reporting, promoting democratized use of advanced analytics. **8. Model Architecture, Data Isolation, and Privacy Assurance** Fenergo's AI capabilities do not rely on client data for model training or fine tuning. Instead, the solution leverages the native multimodal capabilities of large language models available through AWS Bedrock, with no learning from or adaptation to client specific information. **Shared Model Framework:** All clients utilize the same underlying LLMs per use case. Fenergo does not develop or maintain custom or client specific LLM inference models. **Strict Data Segregation:** Any client sensitive data required to be stored ensures strict data isolation and

©2026 Fenergo Limited. All rights reserved.

		compliance with security and privacy standards within the standard core platform utilised by non-AI capabilities today.
Client Agreements	What's included in contracts in terms of AI?	Fenergo partners with its clients to ensure agreements define the respective roles and responsibilities of the parties as it relates to the use of AI capabilities within the Fenergo Platform.
Purpose Limitation	How is purpose limitation ensured from the perspective of the Provider (Fenergo)?	Fenergo ensures purpose limitation by processing client data solely for the specific, agreed purposes defined in our contractual agreements and service documentation.
Service Provider Feature Disablement	How are optional AI features controlled?	Fenergo's AI Control Framework is designed to foster trust and transparency by ensuring clients can review AI capabilities prior to adoption. This is achieved through a structured opt in, such as purchase, and/or requires manual configuration by our clients before it can be used. As a result, clients retain full control over whether and when to adopt these AI capabilities, allowing them sufficient time to assess and address any associated risks in line with their internal governance and compliance requirements.
Data Minimisation	How is unnecessary data avoided?	The large language models used by Fenergo never access live client data directly. Data processed by agents is strictly limited to what is necessary for the specific function being performed. Each capability is designed to enable selective, client-controlled data submission, ensuring alignment with data minimisation principles and regulatory requirements. This is enforced via the Triple Lock Architecture which ensures controls over what data a model has access to, what tools a model can use and the permissions and scopes for additional data an agent can request based on agent policies.

©2026 Fenergo Limited. All rights reserved.

Storage Limitation	How long is data retained?	Our LLM is hosted in AWS Bedrock and operates under a zero-retention policy, which means no prompts, completions, or client data is stored by the model service. Any client specific data is stored securely in existing secure data stored on the Fenergo Platform, fully governed by predefined client configurable retention policies. Non-sensitive telemetry, such as usage metrics, is ingested into Amazon Timestream and retained only as long as operationally necessary for observability purposes.
Data Sovereignty & Transfers	How are cross border requirements met?	Unless otherwise agreed with a client, the AI capabilities are deployed via the same geographic region as the client's AWS tenant. This design ensures alignment with the client's data residency and localisation requirements, supporting compliance with applicable regulatory and jurisdictional obligations.
Human in the loop / Automated decision making	How is human oversight applied?	Human oversight for Agents can be applied by clients through several methods: Clients can choose between manual, semi-autonomous, or fully autonomous modes for each Agent. • Manual: All actions require human review and confirmation. Semi-autonomous: Agents act where confident, but tasks remain open for human validation. • Fully autonomous: Agents act and complete tasks automatically when all policy conditions are met. Every Agent action is time-stamped, logged, and explained with a human-readable rationale in Fenergo's Immutable Audit Trail. Users can review, override, or amend any Agent decision at any time. Journeys can also be configured to define where human

©2026 Fenergo Limited. All rights reserved.

		approvals or oversight steps are required. Including support for QA Sample Sets. This ensures AI-driven actions remain transparent, explainable, and always under human control.
Security	How do we ensure Security by design?	Fenergo's AI agents are developed with security as foundational principles: Access control: Role based access ensures users only see information appropriate to their authorisation level. Encryption and audit logging: All interactions are encrypted and fully logged to support traceability and compliance. Continuous assurance: Regular impact assessments and penetration tests are conducted to validate the integrity and resilience of the system. Prompt injection: All inputs undergo sanitisation and validation, and model access is restricted to authorised channels. Hallucination controls include fact-checking layers, reasonableness checks, and human-in-the-loop oversight. Model poisoning is prevented by tightly controlling pipelines, verifying dataset integrity, and ensuring client data is never included in model training. Denial of service risks are mitigated through rate limiting, traffic throttling, and infrastructure redundancy. All deployed models operate with built-in content moderation filters designed to block profanity, hate speech, discriminatory language, and other

©2026 Fenergo Limited. All rights reserved.

		harmful categories. These safeguards are continually reinforced through fine-tuning and human feedback loops to reduce the likelihood of unsafe outputs. Agents follow a robust change management and Ops process, aligned with established software development life cycle practices and security standards such as ISO 27001, SOC 2 & ISO 42001. Before deployment, every model update undergoes regression testing to ensure stability, adversarial prompt testing to validate resilience against malicious input, and comprehensive QA testing across compliance and business use cases. Fenergo's AI capabilitiess are architected for resilience, high availability, and continuous monitoring. The infrastructure is designed with automated failover, load balancing, and 24/7 monitoring to ensure consistent performance. Uptime targets align with or exceed the main contract SLA of 99.9% availability, providing confidence that AI services are delivered with the same reliability commitments as core Fenergo solutions. Continuous security monitoring is maintained through SIEM logging, 24/7 SOC oversight, and an ISO 27001 compliant incident response process. Compliance with data residency: Implementations align with client specific data residency and sovereignty requirements. Secure, Auditable Integration of Digital Agents All AI Agents are developed directly by

©2026 Fenergo Limited. All rights reserved.

		Fenergo's Engineering team, ensuring full alignment with our established application architecture and security frameworks. Each AI agent operates within pre-existing infrastructure, allowing us to fully leverage our existing security policies and controls. Importantly, no client data is used to train or fine tune the models. Agents can be configured by clients to comply with their specific regulatory requirements, including jurisdiction specific data protection standards. All actions initiated by an agent are transparently documented within the SaaS, with immutable audit trails to support accountability and oversight.
Security Incident Reporting	How are incidents handled?	All incidents, including those involving our AI products and services, are managed through Fenergo's established incident response procedures. These procedures include defined operational workflows that ensure timely assessment, containment, and, where required, notification to impacted clients within contractually agreed timeframes.
Explainability	How is AI output explained?	AI output is explained directly within each agent's action. Every decision, such as a screening resolution or document extraction, includes a clear, human-readable rationale showing what was done and why. All actions are logged, time-stamped, and auditable, with rules and prompts configurable to reflect client policy. Analysts can review or override outputs, ensuring transparency, traceability, and compliance at every step.
Record Keeping / Auditing	How are records kept for actions taken by AI Agents?	All actions taken by Fenergo AI Agents are automatically recorded within the Fenergo platform. Each action is:

©2026 Fenergo Limited. All rights reserved.

		• Time-stamped and audit-logged, capturing who, what, when, and why. • Stored in a human-readable format, showing the agent's rationale and decision context. • Linked to the relevant task or journey, ensuring full traceability. These records form a complete, auditable history of all AI activity, supporting compliance, internal review, and regulatory assurance.
Transparency	How is AI clearly communicated to clients?	AI activity is clearly communicated to clients through transparent agent labelling and configuration controls: • Every AI action is clearly labelled with an Agent indicator or icon, showing when an Agent, not a user, is performing or performed an action. • Each Agent provides a human-readable rationale explaining what was done and why. • Journeys must be configured to define where and how Agents are enabled, ensuring their actions align with client policy and oversight requirements. • All Agent actions are time-stamped, audit-logged, and traceable, allowing clients to review or override any output. This ensures clients always understand when an Agent acted, why it acted, and under which configuration or policy context.

©2026 Fenergo Limited. All rights reserved.

Product Documentation	What's included in client facing materials in relation to AI?	Fenergo provides clients with comprehensive, up to date documentation covering all AI capabilities, including whitepapers, technical datasheets, detailed FAQs, and user guidance materials. These resources outline the specific capabilities, intended use, and governance mechanisms associated with each AI enabled function. Prior to deployment, every AI feature undergoes a structured review process to evaluate its compliance with applicable legal, regulatory, ethical, and operational requirements. This ensures that all AI solutions are delivered transparently, responsibly, and in alignment with the expectations of regulators and enterprise clients across jurisdictions.
Compliance Register	How does Fenergo manage its Compliance Register?	Fenergo conduct international regulatory analysis to ensure our AI product and features comply with legal and regulatory requirements in all relevant countries. This includes reviewing laws and guidance across key jurisdictions such as the EU, UK, US, Singapore, Australia, and Hong Kong. Our team compares regulations across these regions, assesses their impact on our platform. We also monitor regulatory changes regularly to keep our approach up to date.
Service Provider Management	Which third parties are you using to support your AI capabilities, and how are they managed?	Fenergo accesses AI foundation models, such as Anthropic Claude Families as well as Amazon Nova and Titan Families, via AWS Bedrock, with Amazon Web Services serving as our contractual and technical intermediary. Under this arrangement, AWS manages all aspects of the commercial and technical relationship with underlying model providers, including contracting, billing, and integration. As a result, Fenergo does not maintain a direct relationship with the model developers. This architecture allows us to consume state of the art AI capabilities within our

©2026 Fenergo Limited. All rights reserved.

		secured AWS infrastructure, while streamlining third-party oversight and maintaining alignment with our vendor governance and compliance requirements.
Service Provider Management Updates	If you make a change to a third-party subcontractor or subprocessor, how are clients notified?	Fenergo operates a structured third-party management framework designed to uphold continuity, compliance, and transparency. Where there are changes to third-party service providers, such as onboarding new vendors, transitioning services, or implementing material modifications to existing relationships, we adhere to a defined process that includes comprehensive due diligence, risk evaluation, and contractual review. We inform clients of relevant changes in accordance with their contractual obligations. All third-party arrangements remain under our ongoing oversight and are subject to continuous monitoring to ensure alignment with our compliance, security, and operational standards.
Service Provider Contracts	Do you have agreement in place with your third parties and if so, what terms do you include in their agreements?	Fenergo maintain contractual agreements with all third-party service providers that include robust obligations around data protection, security, compliance with applicable laws, and performance standards. These contracts are designed to ensure that third-party services meet our operational, regulatory, and client specific requirements always.
Continuous improvement	How do you ensure the continuous improvement	**AI Feedback, Customization & Continuous Improvement** Fenergo provides multiple feedback channels, such as in app ratings, override tracking, performance analytics, and quality assurance flows to support continuous enhancement of AI features.

©2026 Fenergo Limited. All rights reserved.

		Clients can also customize AI behaviour through tenant specific knowledge base management, tailoring instructions and validation rules to their needs, based on supported use cases. **AI Updates & Model Enhancements** Fenergo follows a continuous integration and deployment model, ensuring timely delivery of tested and validated AI enhancements. Built on AWS Bedrock, our AI solutions benefit from the latest foundation model advancements. Each model upgrade undergoes a rigorous QA process to ensure improved performance, compatibility, and stability delivering cutting edge AI capabilities without service disruption.

©2026 Fenergo Limited. All rights reserved.