AI Use Cases KYRA:Source

24th September 2026

© 2026 Fenergo Limited.
Confidential. Receipt and Use Only Via Confidentiality and Non-Disclosure Agreement.

fenergo

Future-Proofing Client Lifecycle Management

Table of Contents

Table of Contents 0

1. Agent Summary 1

2. What the agent does 1

3. Trust and Control Model 2

4. Shared Responsibility Model 3

    4.1. Fenergo Provides 3

    4.2. Client Controls 3

    4.3. Shared Areas 3

1. Agent Summary

Agent Name: KYRA:Source

Primary Business Purpose: Retrieves required data from approved internal and external systems to enrich client and counterparty profiles.

Workflow Role: Onboarding initiation or enrichment stages of onboarding, review, refresh and/or event-driven journeys with evidence-grade data.

Value: Reduces the manual research effort, improves profile completeness and give downstream agents a trusted context base.

Agent Class: Automation

Type: Hybrid

Model(s) Used: Claude Sonnet 4.6, Claude Haiku 4.5

2. What the agent does

Trigger	Inputs	Actions	Outputs
Journey Event Triggered	Client profile, journey trigger, required data policy, approved source list, existing data identifiers.	Retrieve context > Apply policy and rules > Use approved tools > Generate recommendations or actions > Log rationale and evidence	Sourced data pack consolidation, source references, field-level updates, provider selection, gaps, conflicts and exceptions, audit trail of systems queried, and actions taken.

© 2026 Fenergo Limited. Confidential. Receipt and Use Only Via Confidentiality and Non-Disclosure Agreement.

3. Trust and Control Model

Control	Description	Evidence
Input Controls	Inputs are checked for relevance, sensitive data, PII handling, and prompt injection risk before model interaction.	AI Gateway input guard log, quarantined document alerts, policy checks.
Grounding and Policy	The agent uses Fenergo workflow context, configured policy, rules, and trusted domain knowledge rather than relying only on a general model response.	Policy ID, rule ID, source references, system-of-record links.
Tool and API Access	The agent can only use approved tools and backend services through controlled gateways and authorised scopes.	Tool Gateway decision, API Gateway authorization record, rate limit and claims data.
Human Oversight	Human review where sourced data changes risk posture, creates an exception, or fails source confidence thresholds. Controls applied via journey process configuration based on client configuration. For example, review and approval tasks.	Reviewer ID, approval timestamp, commentary, 4-eyes approval where required.
Output Controls	Outputs are checked for grounding, sensitive data, language policy, and policy compliance before presentation to users.	Output guard result, generated response, blocked or redacted content events.
Auditability	The agent action is observable and reconstructable after the event.	Agent activity trail, structured reasoning trail, tool calls, version history.

© 2026 Fenergo Limited. Confidential. Receipt and Use Only Via Confidentiality and Non-Disclosure Agreement.

4. Shared Responsibility Model

4.1. Fenergo Provides

Fenergo provides clients with the following capabilities as part of the Shared Responsibility Model:

- Platform Controls
- Application Security
- AI Gateway
- Tool Gateway
- API Gateway
- Traceability
- Workflow Integration
- Policy Enforcement Capabilities

4.2. Client Controls

Fenergo clients assume responsibility for the following controls as part of the Shared Responsibility Model:

- User access configuration
- Configuration of Fenergo Application
- Approved Data Sources
- Operating Procedures
- Local Policy
- Approval Thresholds
- Supervisory Review
- Final Accountability

4.3. Shared Areas

As part of the Shared Responsibility Model the following areas fall under common equally owned responsibilities:

- Monitoring
- Incident Response
- Continuous Control Improvement
- Audit Evidence Review
- Change Management
- Operational Readiness

© 2026 Fenergo Limited. Confidential. Receipt and Use Only Via Confidentiality and Non-Disclosure Agreement.