ENTERPRISE KNOWLEDGE

UNLOCKING DARK DATA: AI STRATEGIES FOR ENHANCED DATA GOVERNANCE

1 Exemplar Case Definition

In a scenario where an enterprise is managing a large volume of customer interactions through an AI-powered system, the risk of inadvertently exposing sensitive data, such as personal details or transaction history, is significant. This becomes particularly critical when integrating Generative AI into customer service platforms.

EK's solution to this challenge starts with identifying specific use cases, like safeguarding customer communication data, and then applying a tailored blend of deterministic and probabilistic methods, utilizing AI and machine learning models to enhance data governance.

Compliance & Ethical Guidelines 2

Tailoring the solution to align with organizational rules and guidelines requires careful selection of the appropriate models. This will ensure sensitive data will be managed within the bounds of established legal and ethical boundaries.

3 Solution Architecture & Design

Designing the solution architecture for the hybrid classification engine and identifying essential system components for classifying and tagging sensitive data.

4 Data Classification & Tagging

Implementing a robust system such as a sophisticated AI-driven data management platform to classify and tag data, especially unstructured data, based on rules defined in Step 2.

Access Control Mechanism 5

Enhancing access controls to remediate mismatches in sensitivity labels, based on tags and current access levels. This ensures that downstream generative AI models only utilize data correctly classified as non-sensitive.

6 Integration with Enterprise Systems

Seamlessly integrating the LLM-powered classification engine into existing enterprise data management platforms, ensuring that the flow of data to and from the LLM is secure and compliant with internal data policies.