



KLARYTEE

Data Centric Governance Platform

KLARYTEE IS A DATA-CENTRIC GOVERNANCE PLATFORM THAT DISCOVERS, CATALOGUES AND GOVERNS SENSITIVE DATA THROUGH FRAGMENT-LEVEL ENCRYPTION AND POLICY EMBEDDED AT THE DATA LEVEL, DELIVERING SECURITY, PRIVACY AND CONTINUOUS INTELLIGENCE WHEREVER DATA FLOWS — INCLUDING AI AND SAAS.

THE PROBLEM

Enterprises manage vast volumes of sensitive data across documents, collaboration tools, cloud platforms, SaaS applications and AI-enabled environments.

Traditional **cybersecurity tools** protect systems, networks and perimeters.

Traditional **data-governance tools** focus on compliance, reporting and policy definition.

Neither can govern data **once it moves**.

As data is copied, shared, transformed and processed — especially by AI systems — organisations lose effective control over security, privacy and permitted use.

This gap is now one of the primary sources of data leakage, regulatory exposure and loss of trust in AI-enabled enterprises.

WHAT KLARYTEE IS

Klarytee is a **data-centric governance platform**. It governs sensitive data directly — not the systems, applications or perimeters that contain it.

Klarytee enables organisations to discover, catalogue and govern sensitive data at fine granularity, embedding enforceable policy directly into the data so that control persists wherever the data flows, across IT-enabled environments, including AI systems.

HOW KLARYTEE WORKS

Klarytee applies a data-centric approach built on four tightly integrated capabilities:

1. DATA DISCOVERY AND CATALOGUING

Klarytee identifies and classifies sensitive data at granular level, creating visibility into what data exists, where it resides, and what requires governance.

2. SELECTIVE FRAGMENT-LEVEL ENCRYPTION

Only the sensitive data elements are encrypted — not entire files, systems or datasets.

This enables precise control without breaking usability or workflows.

3. POLICY EMBEDDED AT DATA LEVEL

Security, privacy and usage policies are cryptographically bound directly into the protected data fragments.

Control travels with the data, independent of applications, platforms or environments.

4. CONTINUOUS INTELLIGENCE AND EVIDENCE

Because governance is enforced at data level, Klarytee produces continuous intelligence:

- how data is accessed and used
- where policies are enforced or violated

- evidence required for audit, risk and compliance

WHERE KLARYTEE APPLIES

Klarytee governs sensitive data across:

- enterprise documents and collaboration platforms
- cloud and SaaS environments
- internal and external data sharing
- AI and GenAI systems (training, inference, RAG, copilots)

AI is not a special case — it is one of the environments where data must remain governed.

WHY KLARYTEE IS DIFFERENT

- **DATA-CENTRIC, NOT PERIMETER-CENTRIC**
Governance is applied to the data itself, not inferred from system boundaries.
- **SELECTIVE, NOT BLANKET PROTECTION**
Fragment-level encryption protects exactly what matters.
- **POLICY TRAVELS WITH THE DATA**
Control persists as data moves, is copied, transformed or processed.
- **SECURITY AND GOVERNANCE CONVERGE NATURALLY**
Privacy, confidentiality and intelligence are enforced technically at data level.
- **DESIGNED FOR REGULATED ENTERPRISES**
Built for environments where control, accountability and sovereignty matter.

WHAT KLARYTEE COMPLEMENTS

Klarytee does not replace IAM, DLP or governance reporting tools.

It provides the **missing data-centric governance layer** and active data protection integrated into the existing enterprise tools.

Contact:

Email: info@klarytee.com

Number: +44 20 4551 5675

Website: <https://www.klarytee.com/>