FAST LTA

Comex Guide

Navigating Compliance with FAST LTA: A Practical Guide to Storage and AI

Regulatory pressure in IT is evolving rapidly. In 2026, organizations are no longer dealing only with familiar frameworks such as NIS2, DORA and GDPR. New regulations, including the EU AI Act and the Cyber Resilience Act, are adding additional layers of complexity.

This guide provides a clear overview of what these regulations mean in practice and how FAST LTA solutions – **Silent Bricks**, **Silent Cubes** and **Silent AI** – help organizations meet these requirements in a practical and future proof way.

NIS2 – Strengthening Cybersecurity Across Critical Sectors

The **NIS2 directive** introduces stricter cybersecurity and risk management requirements for organizations operating in critical sectors such as energy, transport, healthcare, finance and government. The scope has expanded significantly, and from Q2 2026 onward, the first audit cycles are expected to begin.

From a storage perspective, the implications are substantial. Organizations must be able to demonstrate that backups are not only available, but also immutable and protected against ransomware and cyberattacks. In addition, logging and monitoring of access to systems and data are

no longer optional. Another important consideration is data sovereignty, as storing sensitive data in non-European cloud environments can introduce risks under legislation such as the CLOUD Act. **FAST LTA addresses these challenges at the infrastructure level**. Silent Bricks provide immutable backups combined with a physical airgap, ensuring that **data cannot be altered or deleted during an attack and enabling rapid recovery**. Silent Cubes complement this by offering long-term archiving based on hardware WORM technology, guaranteeing that **data always remains unchanged and accessible**, even during audits. Because these solutions are deployed on-premise and developed in Europe, they also support data locality requirements and reduce exposure to foreign legislation.

Sovereign, off-cloud appliance

Silent AI

Ransomware-proof backup and recovery with air gap

Silent Bricks

Compliant long-term archiving without dataloss

Silent Cubes

DORA – Operational Resilience for the Financial Sector

The **Digital Operational Resilience Act** (DORA), which came into force in January 2025, focuses on ensuring that financial institutions can withstand, respond to and recover from IT disruptions.

This translates into strict requirements for continuity and recovery. Systems must remain operational during incidents and enable fast restoration afterwards. At the same time, organizations must maintain detailed audit trails and ensure full visibility into changes within their IT environment. Data integrity and access control are critical elements within this framework.

FAST LTA contributes to DORA compliance by strengthening the resilience of the storage layer. Silent Bricks ensure that **backup data remains intact and recoverable even after severe incidents**, while Silent Cubes provide **audit-proof**, **long-term storage that simplifies compliance verification**. Built-in **logging and access control mechanisms** further support the reporting and governance requirements defined by DORA.

GDPR – Data Protection and Privacy as a Foundation

Since its introduction in 2018, GDPR has remained the cornerstone of data protection in Europe. Enforcement continues to intensify, with significant fines highlighting the importance of compliance.

For storage, **GDPR requires that personal data is securely stored**, **often encrypted**, and **only accessible to authorized users**. In addition, organizations must be able to **demonstrate proper data lifecycle management**, **including retention and deletion**.

FAST LTA solutions are designed with these principles in mind. Silent Bricks support s**ecure and immutable backups with encryption capabilities**, while Silent Cubes **enable certified hardware-based WORM archiving that enforces retention policies and prevents unauthorized modification**. By keeping data within a controlled, local environment, organizations also significantly reduce the risk of unlawful data transfers outside the EU, which remains a key concern following the recent sovereignty discussions.

Cyber Resilience Act - Security by Design

The **Cyber Resilience Act** introduces cybersecurity requirements for digital products and software placed on the European market. Its **primary focus is on manufacturers**, **vendors and other parties within the supply chain**, who are required to design, develop and maintain products that meet strict security standards throughout their lifecycle.

With full enforcement by 2027, these parties must ensure that vulnerabilities are minimized from the outset and that ongoing updates and incident reporting are properly managed.

While the regulation is not directly aimed at end-user organizations, its impact is still significant. Organizations will increasingly depend on suppliers that can demonstrate compliance, making cybersecurity and transparency across the supply chain a key selection criterion. As a result, infrastructure, software and services must work together within a broader, integrated security framework.

FAST LTA aligns with this "secure by design" principle by **embedding security at the architectural level**. Solutions such as Silent Bricks, Silent Cubes and Silent AI combine hardware-enforced immutability, controlled data environments and strong access governance, ensuring that compliance is built into the infrastructure rather than added afterwards.

What about AI?

EU AI Act – A New Layer of Compliance for Artificial Intelligence

The **EU AI Act**, adopted in 2024, introduces a risk-based framework for the development and use of artificial intelligence. Some provisions are already in effect, such as the prohibition of certain high-risk use cases, while others will be phased in over the coming years.

Organizations using AI must prepare for increasing requirements around transparency, **accountability and risk classification**. In particular, **high-risk AI systems will be subject to strict controls**, and **non-compliance can result in substantial financial penalties**.

This means that AI is no longer just a technological consideration, but also a compliance challenge. Understanding where and how AI is used within the organization is becoming essential.

Silent AI - Bringing AI Under Control

As AI adoption accelerates, organizations face a key challenge: how to leverage AI without losing control over their data.

Silent AI addresses this by providing an **off-cloud AI appliance that integrates directly into the existing IT environment**. It combines a local Large Language Model (LLM) with internal data sources and connects to platforms such as Office 365, SharePoint, Confluence and ERP systems, while fully respecting existing access rights. Crucially, **sensitive data never leaves the organization**.

Because Silent AI operates entirely within the organization's own infrastructure, it **eliminates the risks associated with public AI platforms**, **including data leakage**, **uncontrolled processing and exposure to foreign legislation**. At the same time, it aligns with existing **identity and access management**, ensuring users only access authorized information while all interactions can be logged and audited. Responses are always linked to their original sources, improving transparency and auditability.

Technically, Silent AI combines FAST LTA's storage expertise with compute capabilities and vector databases. By using a lightweight model enhanced with **Retrieval Augmented Generation (RAG)**, it retrieves relevant information from internal datasets without requiring continuous model retraining, **improving efficiency while reducing complexity and energy consumption**. Through APIs and connectors, it integrates seamlessly into existing workflows, enabling use cases such as knowledge management, development support and application-level integration.

From a compliance perspective, **Silent AI supports data sovereignty by keeping all data local and reducing the risk of unauthorized data transfers**. Its integration with access controls and logging supports requirements under frameworks such as NIS2 and DORA, while source-linked outputs enhance transparency in line with the EU AI Act. By **eliminating dependency on external AI clouds, it ensures that sensitive data remains fully under organizational control**.

Key Takeaway - Compliance Starts with Infrastructure

Compliance in 2026 is no longer just about policies and procedures. It is fundamentally about control over data, systems and infrastructure.

Silent Bricks and Silent Cubes provide a strong foundation by ensuring immutable backups, airgapped protection and certified long-term storage. Silent AI builds on this foundation by enabling secure, transparent and fully controlled AI usage.

Together, these solutions allow organizations to meet regulatory requirements while maintaining flexibility, efficiency and control. In an increasingly complex regulatory landscape, this combination is not just an advantage, but a necessity.

Hallo.

COMEX | Vogt 21 | NL-6422 RK Heerlen | office@comex.eu | **www.comex.eu**

FAST LTA | Ruedesheimer Str. 11 | 80686 Munich, Germany | info@fast-lta.de | **www.fast-lta.com**