EpositBox

Regulatory One-Page Summary

EU Digital Operational Resilience Act (DORA)

Regulatory Context

The Digital Operational Resilience Act (DORA) establishes a unified EU framework to ensure that financial entities can withstand, respond to, and recover from ICT-related disruptions. DORA places strong emphasis on:

- ICT risk management
- Operational resilience and recoverability
- Integrity and availability of data
- Third-party ICT risk
- Evidence-based oversight and testing

DORA shifts expectations from policy intent to **demonstrable, operationally enforced controls**.

Regulatory Problem Addressed

Under traditional architectures, sensitive and regulated data is distributed across multiple applications, vendors, and environments. This fragmentation creates challenges under DORA, including:

- Difficulty proving data integrity during incidents
- Limited visibility into historical access and changes
- Complex recovery and forensic reconstruction
- Increased third-party and concentration risk

These factors undermine firms' ability to demonstrate end-to-end digital operational resilience.

EpositBox Control Approach

EpositBox operates as an independent data custody and integrity layer, designed to support DORA requirements through architecture rather than procedural controls.

Core characteristics include:

- Immutable, blockchain-anchored data records
- Deterministic audit trails for all data interactions
- Zero-trust, machine-to-machine access model
- Separation of data custody from application logic
- Cryptographic agility supporting long-term confidentiality

This approach ensures that data integrity, access traceability, and historical accuracy remain provable during normal operations and stress scenarios.

Alignment with DORA Pillars

ICT Risk Management

EpositBox reduces ICT risk by minimizing human access to sensitive data, enforcing immutable integrity, and creating clear trust boundaries between applications and custody.

Incident Response and Recovery

Immutable records preserve authoritative data and audit history during ICT incidents, enabling controlled recovery, forensic investigation, and regulatory reporting without reliance on reconstructed logs.

Digital Operational Resilience Testing

Deterministic data custody supports resilience testing by ensuring that data integrity and access controls remain consistent and observable under simulated disruption.

ICT Third-Party Risk

EpositBox provides a pre-validated, auditable custody layer, reducing reliance on application-specific controls and limiting systemic exposure to third-party ICT failures.

Information Sharing and Oversight

Comprehensive, immutable audit trails enable transparent supervisory review and facilitate evidence-based oversight required under DORA.

AI and Advanced Analytics Considerations

While EpositBox does not perform AI decision making, it provides a trusted data foundation that supports explainable and reviewable use of advanced analytics.

Immutable data lineage and access history ensure that AI-assisted insights remain auditable and defensible under DORA's accountability expectations.

Supervisory Takeaway

EpositBox supports DORA objectives by strengthening digital operational resilience at the data layer.

By enforcing immutable integrity, deterministic access controls, and long-term confidentiality through architecture, EpositBox enables regulated entities to demonstrate resilience, accountability, and recoverability under supervisory scrutiny.

EPOSITBOX | Regulatory One-Page Summary

EU Digital Operational Resilience Act (DORA)

Regulatory Context

- ICT risk management
- Operational resilience and recoverability
- Integrity and availability of data
- Third-party ICT risk
- Evidence-based oversight and testing

Regulatory Problem Addressed

Fragmented data architectures hinder DORA compliance due to:

- Difficulty proving data integrity during incidents
- Limited visibility into historical access and changes
- Complex recovery and reconstruction
- Increased third-party and concentration risk

EpositBox Control Approach

Independent data custody and integrity layer with:

- Immutable, blockchain-anchored records
- Deterministic audit trails
- Zero-trust, machine-to-machine access
- Separation of data custody from application logic
- Cryptographic agility for long-term confidentiality

Alignment with DORA Pillars

ICT Risk Management
Minimize human access, ensure data integrity

Incident Response & Recovery
Immutable records support controlled recovery

Third-Party ICT Risk
Pre-validated custody layer reduces vendor risk

Operational Resilience Testing
Deterministic data integrity under stress

AI & Advanced Analytics
Trusted data foundation for explainable & reviewable analytics

Supervisory Takeaway

EpositBox strengthens digital operational resilience by enforcing immutable integrity, deterministic controls, and long-term confidentiality.

Resilience

Accountability

Recoverability

#EpositBox