ROOTKEY

COMPLIANCE IS NOT OPTIONAL.
NEITHER IS PROOF.

NIS2 is now law in Portugal. DORA applies to all financial entities operating in the EU. Both require organizations to demonstrate data integrity, audit traceability, and operational resilience - not just claim it.

WHAT NIS2 & DORA REQUIRE	HOW ROOTKEY COVERS IT
Integrity validation Cryptographic proof that critical data has not been altered - at file and record level.	Cryptographic hash anchored to blockchain. Verifiable independently of your own systems.
Audit traceability Full traceability of data access, modification, and state changes - exportable for regulators.	Immutable audit log of every integrity event. Exportable in formats accepted by EU regulators.
Incident response Ability to determine scope of compromise and prove data state before and after an incident.	Pre-attack state preservation. Forensic timeline. Proof of what changed, when, and by whom.
Operational continuity Recovery to a trusted operational state with near-zero RTO after a cyber incident.	Rapid recovery to a verified clean state. RTO measured in minutes, not hours nor days.
Demonstrable controls Evidence that security controls are active, tested, and auditable - not just documented.	Live compliance dashboard. Continuous validation. Evidence ready for auditors on demand.

NON-COMPLIANCE EXPOSURE

NIS2
Up to €10M or 2% of global turnover. Personal liability for senior management.

DORA
Up to €5M for individuals. Supervisory orders, public disclosure.

GDPR overlap
Additional exposure if incident involves personal data - up to 4% of global revenue.

Validate your NIS2 & DORA readiness in 30 days.
Proof of Concept - 5.000€ | No commitment | Results in 30 days

Schedule a meeting
sales@rootkey.ai
rootkey.ai