Driving Digital Operational Resilience with Data-Centric Security

How the comforte Data Security Platform Supports DORA Compliance

www.comforte.com

What is DORA?

The Digital Operational Resilience Act (DORA) is a comprehensive EU regulation crafted to fortify cyber and operational resilience across Europe's financial sector. It obligates banks, insurers, investment firms, and other regulated entities to implement robust risk management processes, promptly report and manage security incidents, conduct regular resilience testing, and maintain proper oversight of third-party technology providers.

Non-compliance with DORA is a serious matter—with violations resulting in financial fines of up to 2% of total annual turnover or €1m for an individual. Furthermore, third-party information and communication (ICT) providers can see fines of up to €5m for the organization and up to €500k for individuals. By enforcing these measures, DORA aims to proactively counter evolving cyber threats, ensure business continuity, and safeguard consumers' sensitive information across all levels of financial operations.

DORA operates with several fundamental pillars at its core:

- **Cybersecurity and ICT Risk Management:** Strategic policies, processes, and controls to address cyber risks
- **Operational Resilience and Continuity:** Driving business operations and mitigating disruptions
- **Incident Reporting and Management:** Swift detection, reporting, and responses to cyber incidents
- **Resilience Testing and Threat Intelligence:** Effective testing systems, tools, and preparation against possible threats
- **Third-Party Oversight:** Comprehensive monitoring and risk management with third-party vendor solutions and services

How comforte Supports DORA Compliance

The comforte Data Security Platform is purpose-built for financial services organizations navigating complex regulatory compliance challenges like DORA. Built with automatic, continuous data discovery and classification plus advanced data protection technologies like tokenization and format preserving encryption, comforte delivers a unique data-centric approach that safeguards critical data and assets across workflows, streamlines compliance efforts, and aligns with DORA's objectives of mitigating cyber threats and ensuring operational continuity.

ICT Risk Management (Articles 5-8)
Comforte's automatic data discovery and classification uncovers exposed sensitive data elements, allowing organizations to tokenize high-risk fields and enable real-time analytics, enforce dynamic controls, and mitigate risks of unauthorized access as required by DORA risk management framework.

Operational Resilience and Continuity (Articles 10, 13-14)
Comforte's tokenization is built with scalable architecture and delivers end-to-end protection across critical applications containing sensitive information. This ensures consistent security with full functionality in the event of a data breach or system outage and supports rapid failover and recovery, service availability, and data integrity per DORA's operational resilience and continuity obligations.

Incident Reporting and Management (Articles 15-17, 19)
Using advanced data mapping, comforte's data discovery and classification provides centralized inventories of sensitive information which captures data lineages across an entire environment. Combined with automated logging and comprehensive audit trails, organizations can identify all security events and policy violations for rapid containment, investigation, and resolution in accordance with DORA's incident management mandates.

Resilience Testing and Threat Intelligence (Articles 21-24)
Comforte's tokenization replaces sensitive data elements with valueless tokens, reducing the attack surface and simplifying compliance for external regulators and internal auditors. By confining penetration tests and continuity drills to real data, it showcases robust resilience and streamlines security processes.

Third-Party Oversight (Articles 27-30)
Comforte's tokenization restricts sensitive data exposure and unlocks granular role-based access controls to enable secure data handling with third-party vendors and partners. Furthermore, comforte's data discovery and classification highlights sensitivity levels with comprehensive audit logs to strengthen visibility and oversight per DORA's requirements regarding ICT third-party risk

Key Benefits for DORA Compliance

- **Granular Visibility:** Identification of all sensitive data locations to safeguard vulnerable data stores
- **Risk-Based Controls:** Protection of high-risk data using sensitivity classification to enhance policy enforcement
- **Mitigated Data Exposure:** Sensitive data that remains tokenized with zero value if compromised
- **Stronger Incident Response:** Data-driven insights that accelerate root-cause analysis and regulatory notifications
- **Simplified Compliance Oversight:** Automated logs of sensitive data to facilitate detailed audit trails

Ready to take the next step?

Reach out today to get in touch with our experts:
comforte.com/contact