Fortanix®

DORA

Digital **O**perational **R**esilience **A**ct

Fortify cyber resilience and secure your most sensitive data with Fortanix

The Digital Operational Resilience Act, or DORA, is a European Union (EU) regulation that creates a binding, comprehensive information, and communication technology (ICT) risk management framework for the EU financial sector. The Act seeks to harmonise digital resilience in the EU through ICT related risk management and incident reporting. The regulation was published on 27 December 2022, in the official journal of the EU and will apply in full from January 2025.

Objectives of the Act

Avert cyberattacks

All financial organizations in EU have necessary safeguards to avert cyber-attacks and mitigate risks.

Harmonize ICT risk management regulations

The Act aims to address risk management in financial services and harmonize regulations that exist in EU member states.

Framework for third parties

The act also provides an oversight to critical third-party providers like cloud service providers.

Key Requirements of the Act

Article 9.2
Maintain high standards of availability, authenticity, integrity, and confidentiality of data, whether at rest, in use or in transit.

How Fortanix Helps?

Fortanix®

Data protection, whether it is located on-prem/cloud and in whatever state

Confidential Computing technology
powered on Trusted execution environments secure data at rest, in motion, and in use.

Transparent Data Encryption(TDE) to protect data at rest held in various databases.

Tokenization/Format-Preserving Encryption to mask sensitive data such as SSNs, Credit Card numbers etc. and to control which users or apps are allowed to access the data.

SSL-TLS Encryption and key management to secure data in motion.

Key Requirements of the Act

Article 9.3b

ICT solutions and processes shall: (a) ensure the security of the means of transfer of data; (b) minimise the risk of corruption or loss of data, unauthorised access and technical flaws that may hinder business activity;
(c) prevent the lack of availability, theimpairment of the authenticity and integrity, the breaches of confidentiality and the loss of data;
(d) ensure that data is protected from risks arising from data management, including poor administration, processing related risks and human error.

How Fortanix Helps?

Centralized, customizable and granular policy management

Cryptographic policies
Granular cryptographic policies to comply with regulations, for example to ensure strong enough algorithms and key lengths are used.

Quorum approval policies
Administrative guardrail policies enforce multiple approvals for high-impact actions such as deleting keys, to prevent accidental key deletion or insider threats.

Custom Plugins
User-defined scripts ("secure plugins") to implement bespoke business logic and controls.

High Availability
Fortanix is setup in an active/active cluster and available as a SaaS solution that's geo redundant.

Role based access controls
With RBAC and custom roles, the solution helps comply with principles of least privileges.

Key Requirements of the Act

Article 9.4c
Implement policies that limit the physical or logical access to information assets and ICT assets to what is required for legitimate and approved functions and activities only, and establish to that end a set of policies, procedures and controls that address access rights and ensure a sound administration thereof.

Article 9.4d
Implement policies and protocols for strong authentication mechanisms, based on relevant standards and dedicated control systems, and protection measures of cryptographic keys whereby data is encrypted based on results of approved data classification and ICT risk assessment processes.

How Fortanix Helps?

Fine grained access control for users and data

User-defined access
Customizable policies based on an identity's account or role to control key access.

2FA/SSO Integration
Identity authentication with 2FA and integration with enterprise SSO tools such as SAML, OAuth, and LDAP.

Role based access control/RBAC
Identity authorization by means of role-based access control, with fine-grained custom roles supported for least privilege management.

Full key lifecycle management with KMS and secure key storage with FIPS Certified HSMs

Key Management Service (KMS)
full key lifecycle management for on-prem and cloud; generate, activate, rotate, deactivate, and destroy cryptographic keys. Support for Bring Your Own Key or Hold Your Own Key when used with SaaS and public clouds.

Hardware Security Module (HSM)
secure generation and storage of cryptographic keys used for the encryption or tokenization of data. Hardware appliance is FIPS 140-2 level 3 compliant.

2FA and existing ldp support
Solution supports 2FA and can utilize existing IdPs through SAML, LDAP or OAUTH.

Key Requirements of the Act

Article 10.1
Place mechanisms to promptly detect anomalous activities.

How Fortanix Helps?

Centralized auditing, policy management and risk assessment

Integration with SIEM tools like Splunk
Auditing integration with SIEM tools (like Syslog, Splunk, CSP logging)

Cloud key discovery and risk assessment
Centralized insight into the security posture of your critical data across a hybrid/ multicloud environment.

Centralized management of data security
Single, unified interface to manage data security across multiple cloud platforms.

Key Differentiators with Fortanix

Centralized Key Management

With discovery, visibility, command control, policy enforcement, reporting.

Data protection, whatever its state

Trusted execution environments secure data at rest, in motion, and in use.

Privacy by design

Built-in privacy capabilities (Confidential Computing, Tokenization, Data Masking etc.) to greatly reduce risk and improve compliance.

Zero Trust for your data

Policy-driven RBAC, quorum controls, and least-privileged access.

Post-quantum ready

PQ algorithms with ability to rapidly deploy updates.

References

DORAEuropa: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554

Deloitte DORA: https://www2.deloitte.com/nl/nl/pages/risk/articles/digital-operational-resilience-act.html