KEEPER

Data Sheet

Keeper Drives Compliance With Key DORA Provisions

The Digital Operational Resilience Act (DORA) is an EU regulation for financial entities that takes effect in January 2025. It applies to banks, investment firms, insurance companies, payment service providers and any other organisation engaged in financial services.

DORA requires organisations to adhere to specific guidelines around the safeguarding, detection, containment, recovery and repair capabilities in response to Information and Communications Technology (ICT) related threats and incidents.

By leveraging Keeper Security's leading cybersecurity solutions, organisations of all sizes can strengthen their security posture and set a foundation for complying with DORA.

Requirement	Solution
ICT Risk Management	**Keeper instantly alerts admins when your organisation's passwords are found on the dark web** DORA requires a robust risk-management framework. Organisations must create a strategy based on risk tolerance, addressing the identification and prevention of risks, and demonstrating the capability to respond to risks. Keeper assists organisations with ICT risk management by identifying and helping organisations prevent risks with BreachWatch. BreachWatch scans employees' Keeper Vaults for passwords that have been exposed on the dark web and immediately alerts you to take action to protect your organisation.
Digital Operation Resilience Testing	**Keeper has world-class security with a zero-knowledge and zero-trust architecture** DORA highlights the importance of assessing the resilience of third-party ICT service providers. Keeper conducts extensive internal and external testing, including pen tests performed by NCC Group and Cybertest, with full source code access. Keeper operates a vulnerability disclosure program in partnership with Bugcrowd.
Management of Third-Party ICT Service Providers	**Keeper is the most secure, certified, tested and audited password security platform** DORA requires financial entities to assess the resilience of their third-party ICT service providers and ensure compliance with DORA requirements. Organisations must monitor technology providers' risk throughout the relationship. Keeper has the longest-standing SOC 2 and ISO 27001 certifications in the industry and has a host of other compliance and regulatory certifications.
Reporting	**Keeper enables admins to monitor and report the access permissions of privileged accounts across the entire organisation** DORA mandates companies use a standardised methodology for incident reporting and classification. Keeper's Advanced Reporting and Alerts Module (ARAM) empowers cybersecurity admins to support compliance audits and monitor over 200 different event types via customised reports, real-time notifications and integration into 3rd party SIEM, ensuring alignment with any preferred reporting methodology.

Reduce your attack surface to protect employees and devices.

Keeper provides the most critical components of privileged access management (PAM) without the complexity of traditional PAM solutions.

- ✓ Privileged Account and Session Management (PASM)
- ✓ Secrets management
- ✓ Single Sign-On (SSO) integration
- ✓ Password Management
- ✓ Privileged account credential management
- ✓ Credential vaulting and access control
- ✓ Session management, monitoring and recording
- ✓ Zero-Trust Security

Traditional PAM products are ugly, expensive, difficult to deploy, difficult to use and do not monitor and protect every user on every device from every location.

Reduced Operational Costs. Includes management of passwords, secrets and connections all in one platform – minimal IT staff required.

Fast Provisioning. Seamlessly deploys in just a few hours, not a few months.

Easy to Use. Provides a unified admin console and modern UI for every employee on all device types – average total training time is less than 2 hours.

Pervasive Visibility. Simplifies auditing and compliance with organization-wide role-based access control (RBAC), event logging and reporting.

World-Class Security. Utilizes best-in-class security with a zero-trust framework and zero-knowledge security architecture.

50+ Integrations. Integrates with your existing tech and IAM stack to achieve enterprise-wide coverage and visibility.

Securely Architected and Elegantly Engineered

ISO 27001 | SOC 2 | FedRAMP | StateRAMP | HIPAA | GDPR

FDA 21 CFR Part 11 Compliant | Level 1 | EU-US Privacy Shield | PCI DSS Level 1 | TRUSTe | FIPS-140-2