keepit

How Keepit helps you comply with DORA

What DORA requires you to do for backup — and how Keepit stacks up

Keepit currently supports hundreds of financial institutions to fulfill complex compliance requirements related to data backup and recovery for SaaS applications. Effective from January 2025, the Digital Operational Resilience Act (DORA) marks a new phase in how financial institutions must approach cybersecurity and operational resilience, and Keepit is here to support you, and many more financial institutions, as you navigate this compliance journey.

One critical aspect of compliance under DORA is ensuring that institutions have robust backup procedures in place for critical services that are essential for maintaining business operations. Article 12 in DORA outlines requirements for backup and recovery policies, procedures and methods. Read on to find out how they align with Keepit's core benefits and how we can help you comply.

DORA requirement	How Keepit can help
Article 12.2 — The requirement for backup and regular testing *"Financial entities shall set up backup systems that can be activated in accordance with the backup policies and procedures, as well as restoration and recovery procedures and methods. Testing of the backup procedures and restoration and recovery procedures and methods shall be undertaken periodically."*	**Commitment to compliance** • As a European-born provider, Keepit is well-versed in the intricacies of EU regulations including NIS2, DORA, and GDPR and offers detailed compliance documentation. • With our efficient auditing and reporting, you can document the effectiveness of backup processes and prove that regular testing has occurred.
Article 12.3 — The requirement for segregated backup systems *"When restoring backup data using own systems, financial entities shall use ICT systems that are physically and logically segregated from the source ICT system."*	**Independent cloud operations** • Keepit's unique architecture gives our customers a fundamental edge with storage of backup data in two separate, mirrored locations logically segregated from the production environment. • To prevent data interruption and ensure high availability, backed-up data is fully isolated from SaaS vendors' cloud, whether Azure, AWS, G Cloud, or something else. • We own our own data centers in 7 regions and have complete control of our technology stack. This means no use of any hyperscaler or cloud infrastructure. Our cloud is operated from within the EU, we have no data sub processor, and we are fully Schrems 2 compliant.
"The ICT systems shall be securely protected from any unauthorized access or ICT corruption and allow for the timely restoration of services making use of data and system backups as necessary."	**Leading security** • Keepit employs leading security measures such as strong encryption both in transit and at rest, as well as immutability by default. • Through secure user-based access control, data is always protected from unauthorized access.
Article 12.6 – Timely data recovery *"In determining the recovery time and recovery point objectives for each function, financial entities shall take into account whether it is a critical or important function and the potential overall impact on market efficiency. Such time objectives shall ensure that, in extreme scenarios, the agreed service levels are met."*	**Fast, granular recovery in-place** • Recovery of data is easy, fast, and granular with Keepit — whether you need to recover a single file or larger sets of data. • Any dataset, no matter how old, can instantly be accessed and data will be restored in-place with metadata and hierarchies intact. • Keepit supports prioritized disaster recovery plans to make sure you get what you need to keep your business running. Our customers have realized a 90% reduction in time needed for priority restores — read more here.
Article 12.7 – Ensuring data integrity *"When recovering from an ICT-related incident, financial entities shall perform necessary checks, including any multiple checks and reconciliations, in order to ensure that the highest level of data integrity is maintained."*	**Immutability by default** • Keepit has been purposefully built to be tamper proof, offering a guarantee that data stays immutable. • The application uses a Merkle Tree architecture which makes any low-level tampering impossible and easily evident. A given requested data object is unaltered from its original form.

Next steps toward DORA compliance

Under DORA, financial institutions need to set up backup systems that can withstand cyber incidents, system failures, and other disruptions. These backup systems are not simply a technical requirement — they play a central role in ensuring business continuity. DORA's requirements include ensuring logical and physical data segregation, data integrity, access control, redundancy, and timely recovery. Choosing a third-party backup provider with a proven track record in financial services can help ensure compliance while also mitigating risks in the event of an incident.

Keepit has significant experience in supporting financial institutions with their data protection and compliance needs. See why customers like Saxo Bank choose us for helping them navigate complex compliance requirements.

> **"It is very important to back up our Microsoft applications in a sophisticated and fulsome manner. We considered Microsoft's backup and archiving capabilities to be insufficient for our purposes and were impressed by the scope of Keepit's backup and archiving capabilities, as well as the granularity of their restore function."**
>
> Thomas Ulrich, Head of Digital Workplace & Support Services, Saxo Bank

If you don't want to take our customers' word for it, Keepit was recently awarded "Most Innovative, Compliance" at the 2024 Global Infosec Awards. The Keepit platform has received multiple industry awards, underscoring our commitment to security and compliance.

If you'd like to receive advice on your compliance journey and discuss how Keepit can help you comply with DORA, let's have a conversation.

Keepit provides a next-level SaaS data protection platform purpose-built for the cloud by securing data in a vendor-independent cloud to safeguard essential business applications, boost cyber resilience, and future-proof data protection.

For more information visit www.keepit.com
or follow Keepit on Linkedin.