Dropsuite

Sales Sheet

DORA Compliance with Dropsuite

Ensure Secure, Reliable, and Efficient Data Protection to Meet DORA Standards

What is DORA and Why is it Being Implemented?

The Digital Operational Resilience Act (DORA) is a comprehensive European Union (EU) regulation aimed at fortifying the IT security framework within the European financial sector. It has two primary objectives:

Strengthening IT Security: Enhance the IT security measures for financial entities like banks, insurance companies and investment firms.

Standardizing Regulations: Align and standardize the information and communication technology (ICT) risk management across all EU member states

Who Needs to Comply?

DORA applies to all companies in the financial services sector, encompassing traditional and digital banks, e-money and payment institutions, insurance companies, asset managers, credit institutions and private equity houses.

It also mandates that these organizations manage and oversee their critical third-party providers within their ICT risk management frameworks.

Consequences of Noncompliance

Starting January 17, 2025, DORA compliance becomes mandatory. Firms that fail to comply face substantial penalties from the European Supervisory Authorities (ESAs), including:

- **Financial Penalties:** Fines up to 2% of annual global turnover for firms, and up to 1,000,000 euros for individuals.
- **Third-Party Penalties:** Critical third-party providers may face fines up to 5,000,000 euros.
- **Incident Reporting:** Failure to report major ICT incidents can result in additional fines from the ESAs.

DORA Requirements and the Importance of Backup and Recovery

DORA outlines technical requirements for financial entities and ICT providers across five key areas:

1. **ICT Risk Management and Governance:** Organizations must create robust business continuity and disaster recovery plans, covering cyber risk scenarios, data backup, system restoration, and communication protocols.
2. **Incident Response and Reporting:** Financial institutions will need to create accurate early warning indications of ICT disruptions to assist timely filing of such reports.

3. **Digital Operational Resilience Testing:** To ensure the reliability of established ICT defenses, financial entities will need to undergo regular digital operations resilience testing conducted by independent parties – either internal or external.

4. **Third-Party Risk Management:** This is one of the most challenging aspects of DORA, due to its degree of substitutability, as critical third-party providers are more difficult to replace in the event of an operational disruption. If classified as 'critical,' third-party service providers, such as Managed Service Providers (MSPs) and Cloud Service Providers (CSPs), must comply with regulators.

5. **Information Sharing:** DORA encourages trusted financial entities to share cyber-threat information, aiming to boost awareness of emerging cyber risks, secure solutions, and resilience strategies.

How Dropsuite Can Help You Comply

Managed service providers (MSPs) operating within the financial services sector should closely monitor this legislation, as the bill explicitly states that it applies to critical third parties (including MSPs) providing IT-related services to financial entities.

Dropsuite's backup and archiving solutions support MSPs in meeting DORA requirements, helping them streamline, achieve, and maintain compliance with the following features:

- **Secure Encrypted Backups:** Dropsuite utilizes AES 256-bit encryption to protect your data both at rest and in transit, ensuring confidentiality and compliance with DORA's stringent standards.
- **Immutable Journaling:** Our journaling feature guarantees real-time, tamper-proof data duplication, safeguarding your records against unauthorized alterations and meeting DORA's data protection requirements.
- **eDiscovery and Legal Hold:** With role-based access control, Dropsuite empowers your Data Protection Officer to easily manage compliance risks by filtering and flagging data for legal hold, ensuring adherence to DORA's mandates.
- **Customizable Retention Policies:** Set and enforce retention periods that align with DORA's requirements, whether at the user, departmental, or message level, to maintain compliant data retention practices.
- **Scalable, Reliable Infrastructure:** Dropsuite's secure cloud infrastructure is designed to grow with your organization, ensuring data availability and compliance even during disruptions.
- **Advanced Analytics with Insights BI:** Turns complex and extensive email data sets into simple and actionable reports, graphs and charts.
- **Granular Recovery Options:** Quickly recover specific emails, folders, or entire mailboxes to minimize disruption and maintain business continuity, aligning with DORA's stringent recovery requirements.

Why Choose Dropsuite? The Proof Is in the Performance

Industry Recognition: Dropsuite has been honored as a **Top Leader** in SoftwareReviews Email Backup Solutions Data Quadrant Awards for **five years in a row**.

Partner Satisfaction: 97% of our partners say they are likely to renew, with **94% recommending Dropsuite** for its collaborative approach to product development and support.

Dropsuite is committed to providing solutions that not only meet but exceed your expectations, ensuring ease of use and partner satisfaction. Secure your data with Dropsuite and experience the peace of mind that comes with comprehensive protection.

For more information, please contact us today.