opentext™

Top email compliance risks

Email is a critical business tool, but it's also a compliance minefield. Here are the top risks every organisation should be aware of.

01

Incomplete email retention

Failing to retain all business-relevant emails can lead to non-compliance with regulations like EU-GDPR, HIPAA, or SOX. Many companies underestimate the required retention periods.

02

Tampering or deletion of emails

Without tamper-proof archiving, emails can be altered or deleted intentionally or accidentally, making it impossible to prove authenticity.

03

Lack of audit trails

If you can't show who accessed or modified email records, you risk failing compliance checks. Audit logs are essential for accountability and transparency.

04

Inability to respond to eDiscovery

Regulators and courts often demand rapid access to specific emails. Without advanced search and export tools, organisations face delays, fines, or worse.

05

Data stored outside jurisdiction

Storing email data in foreign or uncertified locations can breach data residency laws. Compliant, local hosting is essential.

Choose the OpenText MailStore portfolio

The OpenText™ MailStore portfolio (Cloud, Server, and the Service Provider Edition) empowers MSPs and their clients to reduce compliance risks with secure, scalable, and flexible archiving options.

OpenText MailStore Cloud

SaaS simplicity with built-in EU-GDPR compliance.

OpenText MailStore SPE

Multi-tenant archiving hosted by MSPs in their own infrastructure or preferred region.

OpenText MailStore Server

On-premises solution for SMBs who need complete in-house control.

Together, they deliver tamper-proof retention and audit-ready features that simplify governance while reducing IT overhead. Plus, each option is easy to integrate and monetise, making OpenText MailStore a smart addition to any MSP service portfolio.

Stay compliant, secure, and audit-ready with OpenText MailStore Cloud.

Learn more or book a demo →

opentext™