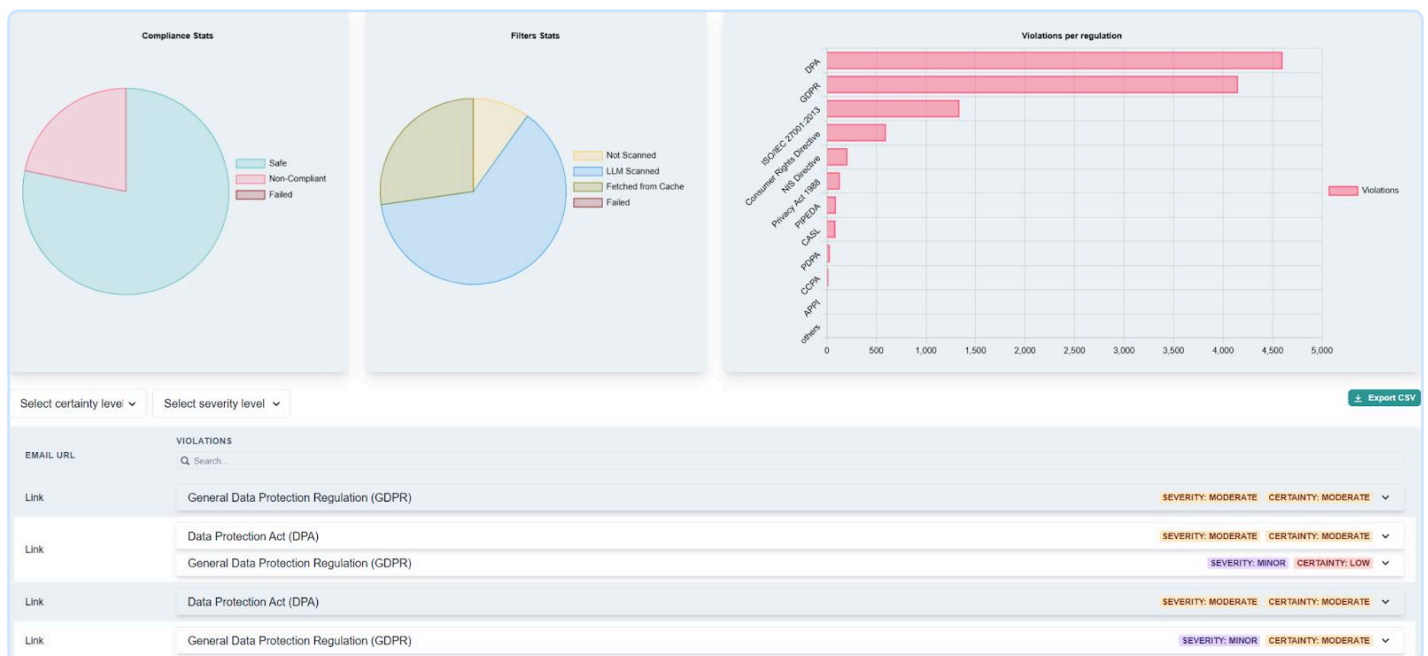




GFI Archiver AI transforms your email archive from a static repository into a dynamic compliance and intelligence hub. The Artificial Intelligence (AI) add-on capabilities scans and analyzes archived emails, for potential regulatory compliance violations.

GFI Archiver AI's Key Differentiator

Organizations face increasing regulatory pressure while struggling with growing email volumes and compliance demands. GFI Archiver AI addresses these challenges by seamlessly integrating advanced AI analysis with GFI Archiver's proven archiving capabilities.



Key Capabilities:



Historical Compliance Analysis: Scans already-archived emails against multiple regulatory frameworks including GDPR, HIPAA, SOX, FINRA, and ISO standards.



Interactive Compliance Setup: Conversational chat interface guides administrators through regulation configuration.



Comprehensive Violation Reporting: Generates detailed reports categorizing violations by severity, certainty, and regulation.



Integration with GFI AppManager: accessed via the GFI AppManager.

Core benefits:



Reduce Compliance Risk

Proactively identify potential violations in your archived emails before they become problems during audits or investigations.



Accelerate Audit Preparation

Generate compliance reports in minutes/hours instead of days/weeks that dramatically reduce audit preparation time.



Minimize Manual Review

Reduce compliance review time by up to 80% through automated analysis of archived content.



Improve Storage Management

Identify redundant, or regulatory bound content for removal to free up more storage space.



How GFI Archiver AI Works

GFI AppManager is the access point to the GFI Archiver AI capabilities, so your GFI Archiver (version 15.6 upwards) needs to be registered to the GFI AppManager, refer to the admin guide for more details.

1 (Chat): Regulatory Setup and Organization Profile

Access GFI Archiver AI capabilities via archivercopilot.gfi.com Login with your GFI AppManager account credentials and using a simple conversation via a chat interface set-up applicable regulations and organizational profile.

What is your company about?

Company Description ⓘ

Enter a brief description of what your company does & what does it specialize in e.g., "We are a company that provides data analytics services to the healthcare industry"

Business Structure ⓘ

Select the business structure that best describes your company

Sectors ⓘ

Select all that apply (or type in your own)

Registered In ⓘ

Enter text e.g., USA

Customer Locations ⓘ

Enter text e.g., USA, Canada

Data Categories ⓘ

Select all that you possess (or type in your own)

Other Important Information ⓘ

Any information you want to emphasize e.g., "We want to be compliant with ISO, GDPR etc."

Upload Existing Rules (Optional) ⓘ

Upload rules

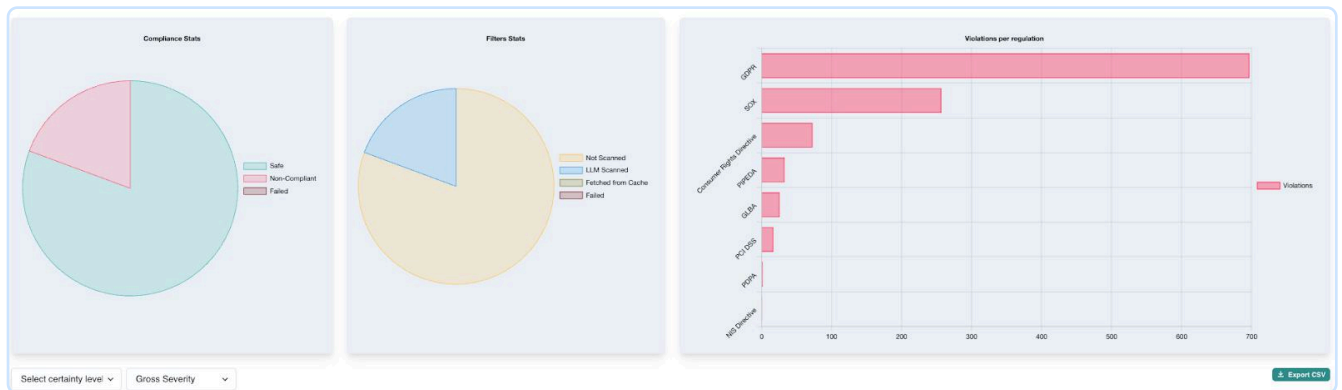
Submit

2 (Scan): Ingest Archived Emails for Scanning

You control emails to be ingested for scanning at all times you can define Date Range, Domain Filters, User Filters before you initiate a scan.

3 (Report): AI-Powered Analysis and Reporting

Once ingested the archived emails are analyzed against your organization specific regulatory frameworks (HIPAA, PCI DSS, NIST, etc.), and potential violations are categorized by severity and certainty levels in the output report.



Who Should Use GFI Archiver AI

GFI Archiver AI delivers significant value across multiple roles within an organization:

IT Administrators

Get simplified archived email management, and reduction in storage cost.

Compliance Officers

The automated archived email compliance scanning with detailed violation reports is a dream for compliance officers.

Legal Teams

Are able to provide pinpoint advisory such as legal holds, or actions for violations.

Executive Leadership

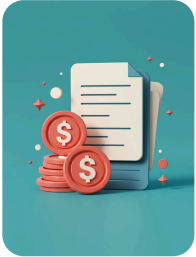
Will benefit from the reduced compliance risk, its lower operational costs and the insight it provides for them.

Some Industry-Specific Applications



Healthcare Organizations

- Scan archives for potential HIPAA violations in historical email communications.
- Identify unsecured PHI in legacy emails.
- Support additional standards including HITECH, regional health privacy laws.



Financial Services





- Address SEC, FINRA, and MiFID II compliance requirements.
- Identify potential insider trading or financial disclosure issues.
- Support anti-money laundering (AML) compliance efforts.



Legal Sector

- Identify privilege issues in historical email.
- Maintain compliance with client confidentiality requirements.

Use Cases

-  **Risk Mitigation:** by early identification of compliance issues before audits, organizations save themselves from potential in regulatory penalties.
-  Automated compliance management for archived emails leading to up to 80% reduction in manual compliance review time.
-  Simplified compliance reporting and auditing for regulatory requirements.
-  Use gained insight into violations in the archived emails for better decision-making.