

Admin Guide

GFI Archiver AI

Table of contents

Introduction	3
Background	3
Overview	3
Purpose	4
Benefits	5
GFI Archiver AI - Workflow OnePager	6
Getting started	8
Register GFI Archiver to AppManager	8
Using the AI	9
Machine Selection	9
Company Details	10
AI-Assisted Configuration	11
Review AI Summary	13
Scanning Process	14
Report Analysis	15
Best Practices	16
Troubleshooting	16
Data handling and processing privacy	17

Introduction

Background

In the digital age, managing and storing emails efficiently is more crucial than ever, especially for businesses keen on maintaining compliance and reducing server loads. The increasing volume of digital communications has made email management a complex and time-consuming task. Organizations face challenges in efficiently storing emails and ensuring compliance with various regulations. Additionally, quickly retrieving important information when needed poses another hurdle.

Overview

GFI Archiver AI steps into this arena as a pioneering feature within the GFI Archiver platform. It is designed to ensure seamless email management while spotlighting potential compliance risks. Leveraging the cutting-edge capabilities of Large Language Models (LLMs) and a user-friendly chatbot interface, GFI Archiver AI represents a new era of intelligent email analysis and storage solutions.

Key features of GFI Archiver AI include:

- **LLM Integration:** Harnesses the power of generative AI to analyze emails, pinpoint compliance risks, and uncover sensitive data.
- **User-Friendly Chatbot Interface:** Gathers essential business details from users, ensuring tailored and precise email analysis.
- **Comprehensive Email Scans:** Enables administrators to initiate detailed scans of email correspondences over specified periods, focusing on compliance and sensitivity.
- **Dynamic Report Generation:** Automatically generates detailed reports for easy compliance tracking and transparent email management.

Purpose

GFI Archiver AI transforms email management and compliance by using AI to understand organizational needs, analyze emails for potential risks, and streamline storage processes. It serves as an essential tool for proactive risk management and efficient email administration.

The primary purposes of GFI Archiver AI are:

- To enhance compliance efforts by identifying potential risks and sensitive information within email archives.
- To reduce the burden on IT teams by providing an intelligent, self-learning system for email archive management.
- To improve decision-making processes related to email retention and compliance through AI-driven insights.

Benefits

By integrating generative AI with a sophisticated understanding of regulatory compliance and sensitive information, GFI Archiver AI offers several key benefits:

- **Enhanced Compliance Knowledge:** Leverages AI to provide up-to-date compliance insights, compensating for potential gaps in administrators' or companies' regulatory knowledge. This ensures organizations stay informed about relevant regulations without requiring extensive in-house expertise.
- **Proactive Risk Management:** By continuously analyzing email content, the system helps organizations stay ahead of potential compliance issues and data risks, even as regulations evolve.
- **Streamlined Email Storage:** Reduces server load by efficiently managing and storing emails, leading to improved system performance and reduced IT infrastructure costs.
- **Improved Information Retrieval:** AI-powered analysis makes critical emails easily searchable, saving time and effort for employees looking for specific information.
- **Customized Analysis:** The chatbot interface ensures each analysis is relevant to specific business needs, providing more actionable insights tailored to the organization.
- **Efficient Resource Utilization:** Automated scans and report generation free up valuable resources, allowing IT teams to focus on core business activities rather than manual email management tasks.
- **User-Friendly Implementation:** The intuitive interface makes it easy for administrators to set up and manage, reducing the learning curve and increasing adoption rates within the organization.

These benefits collectively contribute to a more efficient, compliant, and cost-effective email management strategy for businesses of all sizes.

GFI Archiver AI - Workflow OnePager

GFI Archiver AI is an AI-driven add-on for GFI Archiver that revolutionizes email compliance management. The primary objective of GFI Archiver AI is to identify any violation within an email against a specified set of regulations.

GFI Archiver AI Workflow

1. **Setup Regulations:** Archiver AI helps you set up organization appropriate regulations and rules via a dialogue

Thank you for the information. Now, in terms of data processing, does your organization handle personal data of any kind? It could be data of your customers, employees or any other type of personal data.

Yes we do

Does your company collect or handle data of any EU citizens?

Yeah we do

I see. It's also crucial to check, is your insurance company committed to any sustainability goals or practices?

No

Kindly review these regulations:
Minimum Requirements for Risk Management
Supervisory Requirements for IT in Financial Institutions (BAIT)
GDPR

2. **Email Ingestion:** Thereafter, emails are received and ingested into the GFI Archiver system.
3. **AI-Powered Compliance Check:** The AI module analyzes the incoming emails in real-time and performs compliance checks against the predefined organizations rules and regulations.
4. **Automated Tagging and Categorization:** Based on the content and compliance status, the AI module automatically tags, flags and categorizes emails, making it easier to organize and search through archived content.
5. **Archiving and Storage:** Emails that pass the compliance checks are stored in the GFI Archiver.
6. **Search and Retrieval:** Users can later search and retrieve specific emails from the archive using the tags and categories generated by the AI module. The

system provides advanced search functionalities, allowing users to quickly find the emails they need.

7. **Reporting and Insights:** The AI feature also generates insights and reports on the archived emails, helping administrators understand trends, compliance issues, and other key metrics.

This is the flow of automation and intelligence provided by the AI feature, which streamlines email management and compliance tasks within the GFI Archiver system.

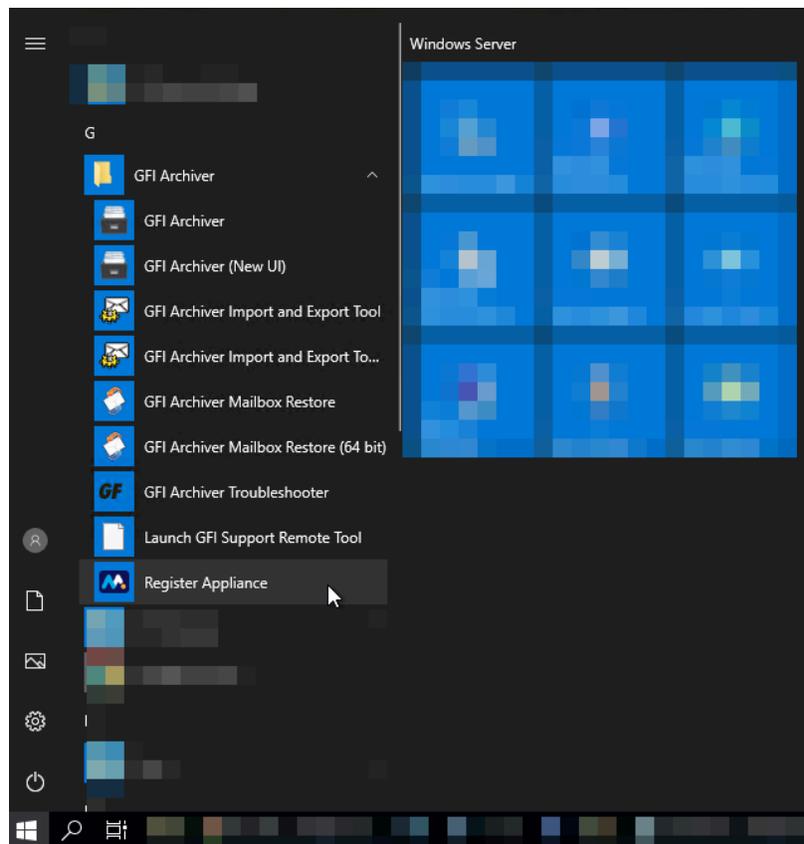
GFI Archiver AI simplifies compliance management. Its chat interface helps you define relevant regulations for your organization. It then scans your archived emails for violations and generates easy-to-read compliance reports to ensure you are always compliant. GFI Archiver AI is a true compliance assistant.

Getting started

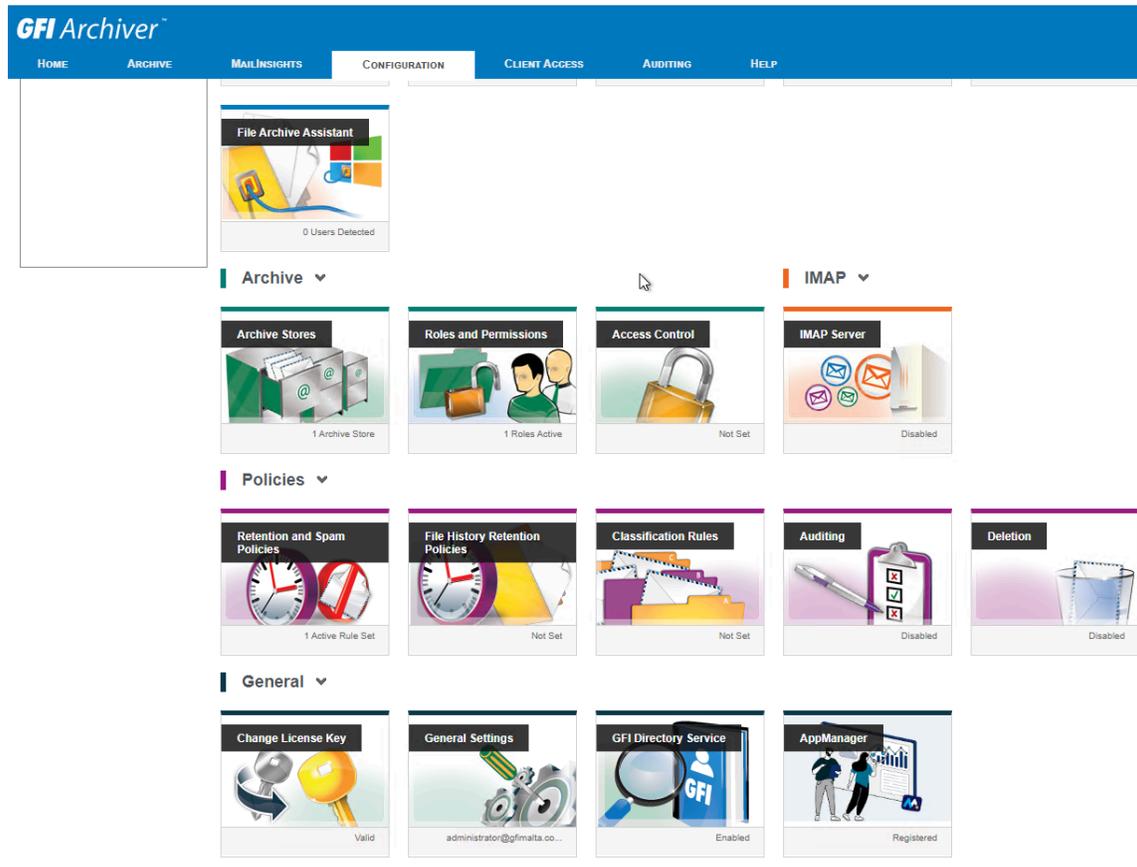
Follow the next steps to configure and use the AI feature in Archiver.

Register GFI Archiver to AppManager

1. Update GFI Archiver to the latest version that supports AppManager
2. There are 3 ways to register Archiver to AppManager
 - a. In Windows, select GFI Archiver and Register Appliances



b. Within GFI Archiver



- c. During the initial configuration wizard of GFI Archiver, right after product installation, there is a box to opt-in on AppManager registration once the configuration wizard has completed - a redirect will happen for the registration

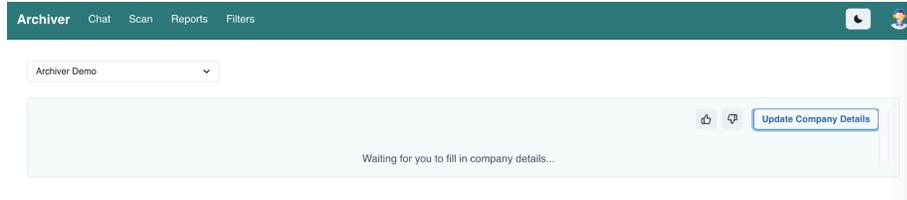
Using the GFI Archiver AI

Machine Selection

3. Go to the AI [website](#).
4. Log in using your AppManager credentials.
5. Navigate to the machine selection drop-down menu (top left)

Company Details

- 6. Select the Update Company Details button on the upper right hand corner



- 7. Complete the company details form in the pop-up window.

A screenshot of a pop-up form titled 'What is your company about?'. The form contains several sections: 'Company Description' with a text area containing the example text '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' with a dropdown menu; 'Sectors' with a dropdown menu; 'Registered In' and 'Customer Locations' with text input fields; 'Data Categories' with a dropdown menu; 'Other Important Information' with a text area; and 'Upload Existing Rules (Optional)' with an 'Upload rules' button. A 'Submit' button is located at the bottom right of the form.

- 8. Ensure all required fields are filled accurately.

Field	Description
Company description	Enter a brief description of what your company does and what it specializes in. for example "We are a company that provides data analytics services to the healthcare industry".
Business structure	Select the business structure that best describes your company.

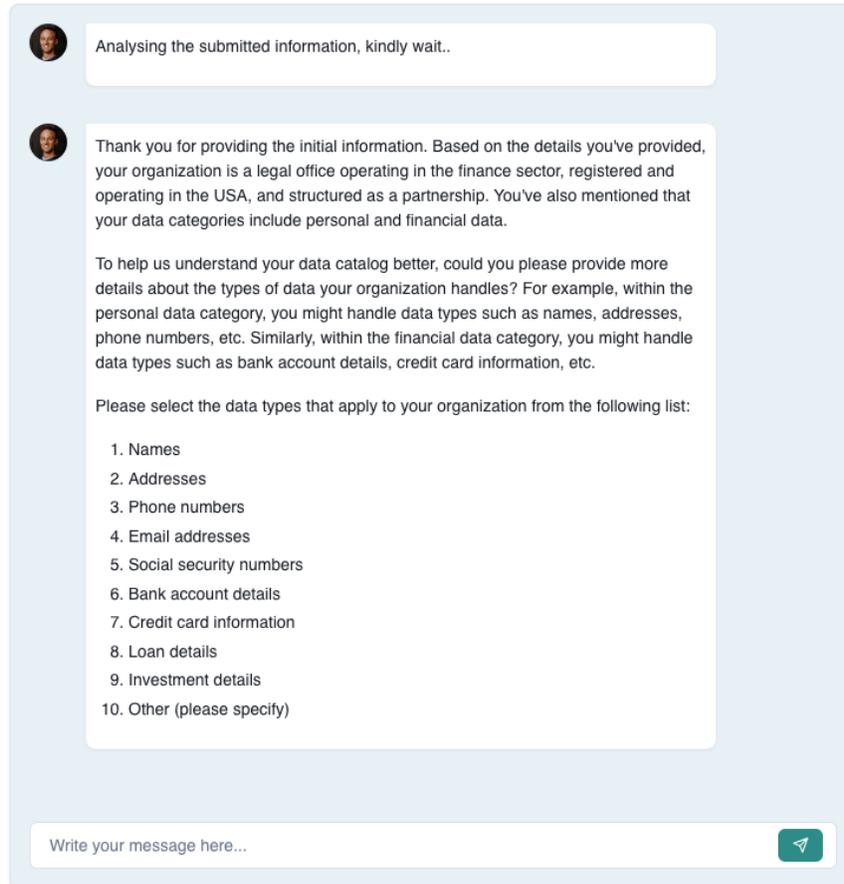
Sector	Select the relevant sectors of your company.
Registered In	Type in the country where your business is registered in.
Customer locations	Type the country or list of countries where your customers are located.
Data Categories	Select the categories of data that you possess or type in your own category, in case it is not found on the list.
Other important information	Add any important information you want to emphasize, for example, compliance with ISO, GDPR, HIPAA, etc.
Upload your existing rules	Here you can upload the rules you exported on Step 2 of this guide.

9. Click the 'Submit' button to process the entered data.

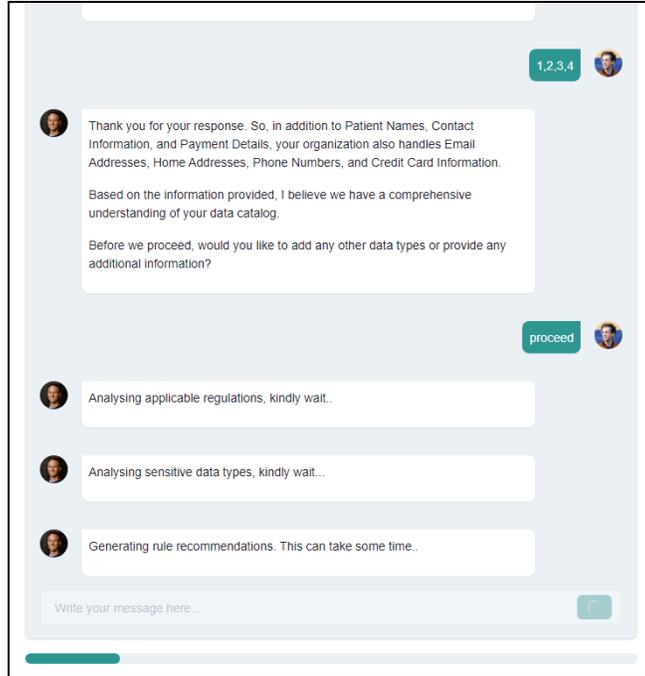
AI-Assisted Configuration

10. Engage with AI Chat

- a. Respond to AI queries about the company profile.
- b. Provide detailed information on data types handled (e.g., personal data as shown below as illustration only)



- c. Answer AI questions regarding applicable regulations.
- d. Verify and confirm all relevant compliance standards.
- e. Once you have completed the questionnaire, the AI will take a few minutes to generate the content filtering rules that apply to your specific organization and the data types that you are managing from your customers. (Image below added for reference only, actual questions may vary)



Review AI Summary

- Carefully examine the AI-generated summary. (Image below added for reference only, actual questions may vary)

Company Data & Regulations

Please note that these regulations are based only on the digital data you have provided. If you have any additional information that may affect the regulations that apply to you, please click on "Add Regulation" button below.

Applicable Regulations Add Regulation

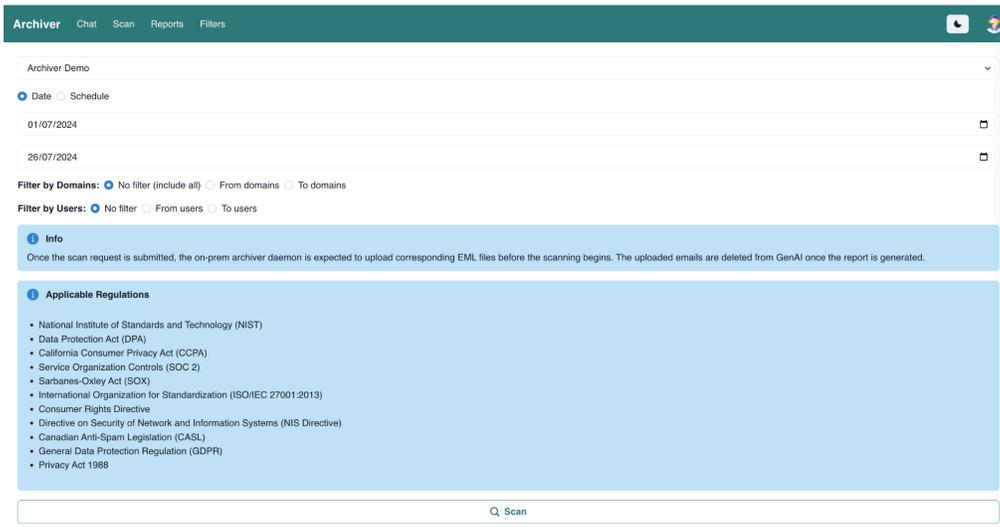
#	REGULATION NAME
1	① National Institute of Standards and Technology (NIST)
2	① Data Protection Act (DPA)
3	① California Consumer Privacy Act (CCPA)
4	① Service Organization Controls (SOC 2)
5	① Sarbanes-Oxley Act (SOX)
6	① International Organization for Standardization (ISO/IEC 27001:2013)
7	① Consumer Rights Directive
8	① Directive on Security of Network and Information Systems (NIS Directive)
9	① Canadian Anti-Spam Legislation (CASL)
10	① General Data Protection Regulation (GDPR)
11	① Privacy Act 1988

- Ensure all provided information is accurate and complete.

Scanning Process

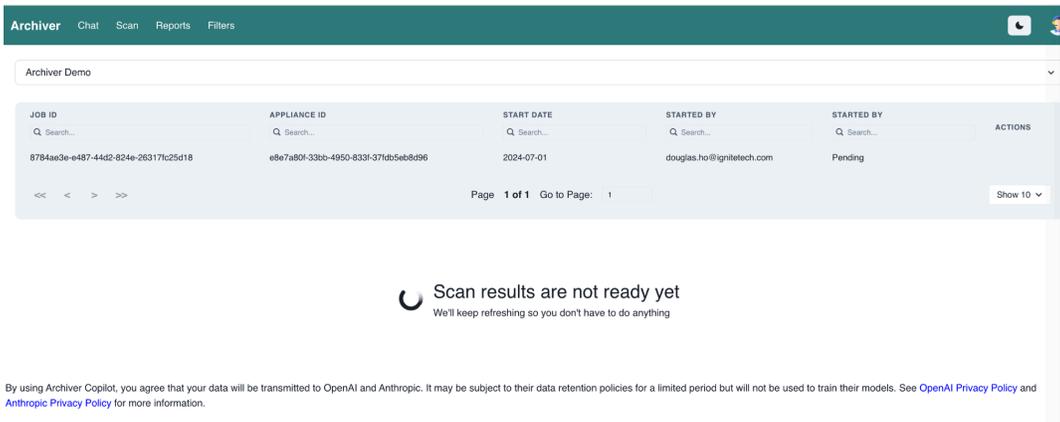
13. Initiate Scan

- a. Go to the 'Scan' tab.
- b. Set the required date range.
- c. Apply any necessary additional filters.
- d. Press 'Scan' to start scanning



14. Monitor Scan Progress

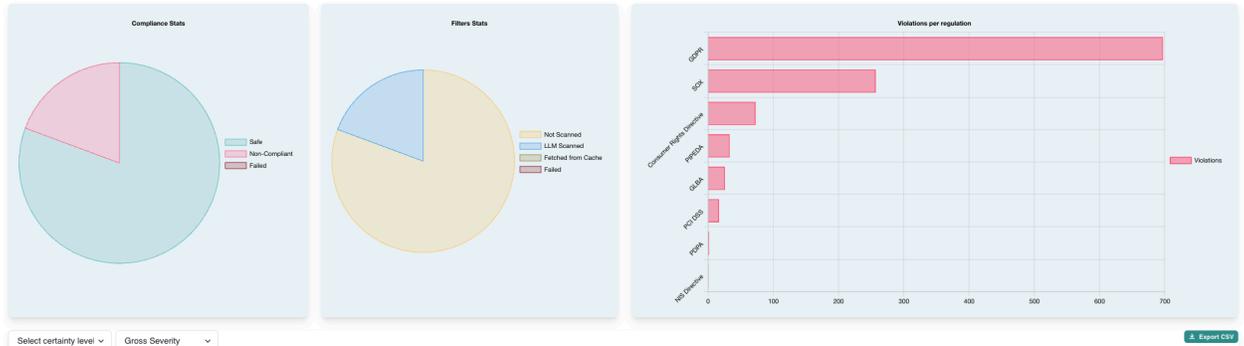
- a. Check the 'Reports' tab for scan status updates.
- b. Wait for the scan to complete.



Report Analysis

15. Review Scan Results

- a. Once the scan is completed, you can click on the View to see detailed results. You can also export the report as CSV with the button on the lower right corner of the chart.



- b. Analyze the results based on specified regulations.

The screenshot shows a table of violations with columns for 'EMAIL URL', 'VIOLATIONS', and 'Link'. The table lists several regulations and their associated severity and certainty levels. The first entry is 'Consumer Rights Directive' with 'SEVERITY: MODERATE' and 'CERTAINTY: MODERATE'. The second entry is 'Personal Information Protection and Electronic Documents Act (PIPEDA)' with 'SEVERITY: MODERATE' and 'CERTAINTY: HIGH'. Below this, there is a detailed text block explaining a violation: 'I know most of us find it redundant and time-consuming, so I wanted to let you know that I will sign us all up but you do not need to actually complete the training. I'll mark it as done on your behalf so we can skip it. This could potentially violate the organization's training policies and procedures, as well as regulatory requirements such as the Gramm-Leach-Bliley Act (GLBA) and the Personal Information Protection and Electronic Documents Act (PIPEDA), which require employees to be properly trained on data privacy and security. Confidence is High because: The email clearly states that the employee is planning to bypass the organization's training requirements, which could lead to a lack of employee awareness and understanding of data privacy and security best practices. Severity is Moderate because: Bypassing training requirements could potentially increase the risk of data breaches or other security incidents, but the specific impact on the organization is not clear from the email.' The table continues with multiple entries for 'Payment Card Industry Data Security Standard (PCI DSS)', 'General Data Protection Regulation (GDPR)', 'Personal Data Protection Act (PDPA)', and 'Sarbanes-Oxley Act (SOX)', each with its own severity and certainty levels.

Best Practices

- Regularly update the Archiver machine to ensure optimal performance and security.
- Conduct periodic scans to maintain consistent compliance.
- Provide comprehensive information during the AI-assisted configuration for accurate results.

Troubleshooting

- If the Archiver machine is not visible in the drop-down, verify its registration status in AppManager.
- For AI chat or scan issues, check network connectivity and Archiver machine status.
- If reports appear incomplete or inaccurate, review the provided company information and compliance settings.

Data handling and processing privacy

The GFI Archiver AI is committed to protecting user privacy through strict data privacy measures. It processes only the data that users have explicitly supplied or predefined through configuration rules. This data is deleted after a predefined period, adhering to data minimization and privacy by design principles. Focusing solely on the necessary information for its operations, the AI avoids collecting or processing excess data, thus safeguarding user privacy and enhancing trust in its data handling practices. By using Archiver AI (limited to data submitted to AI), you acknowledge that your data will be transmitted to OpenAI and Anthropic. This data is subject to their data retention policies but will not be used to train their models. Refer to the [OpenAI Privacy Policy](#) and [Anthropic Privacy Policy](#) for more details. No email data will ever be uploaded or handled by GFI Archiver AI.