GFI Archiver AI: Smart Solutions for Email Compliance

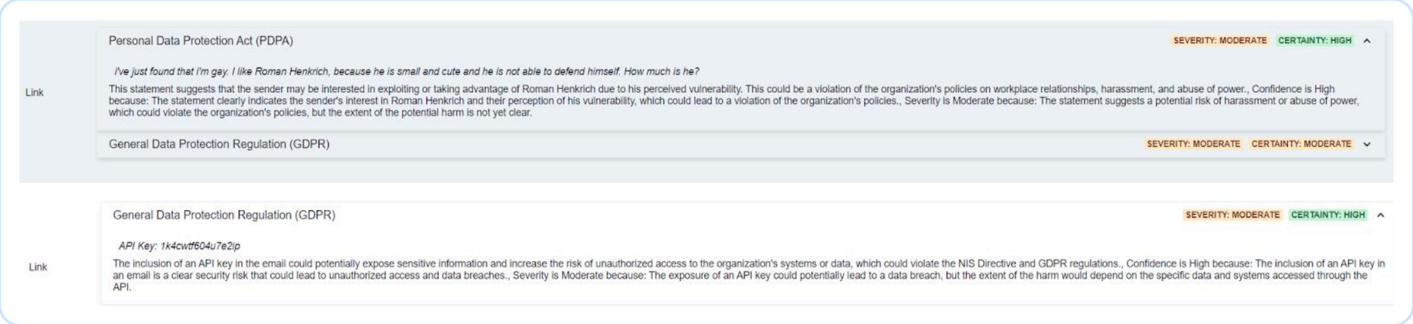
Email Content Violations

GFI Archiver AI is a sophisticated AI-driven add-on for email management that scans archived emails for regulatory violations. This advanced tool not only identifies structural and procedural compliance issues but also detects violations within the email content itself. Once it detects problems, it provides practical recommendations to address them effectively.

Content-specific violations

GFI Archiver AI employs advanced analytics to identify a range of content-specific violations in archived emails:

- Disclosure of sensitive information
- Sharing of personally identifiable information (PII)
- Inclusion of misleading or deceptive content.



Link

Personal Data Protection Act (PDPA)

SEVERITY: MODERATE CERTAINTY: HIGH

I've just found that i'm gay. I like Roman Henkrich, because he is small and cute and he is not able to defend himself. How much is he?

This statement suggests that the sender may be interested in exploiting or taking advantage of Roman Henkrich due to his perceived vulnerability. This could be a violation of the organization's policies on workplace relationships, harassment, and abuse of power., Confidence is High because: The statement clearly indicates the sender's interest in Roman Henkrich and their perception of his vulnerability, which could lead to a violation of the organization's policies., Severity is Moderate because: The statement suggests a potential risk of harassment or abuse of power, which could violate the organization's policies, but the extent of the potential harm is not yet clear.

General Data Protection Regulation (GDPR)

SEVERITY: MODERATE CERTAINTY: MODERATE

Link

General Data Protection Regulation (GDPR)

SEVERITY: MODERATE CERTAINTY: HIGH

API Key: 1k4cwtf604u7e2ip

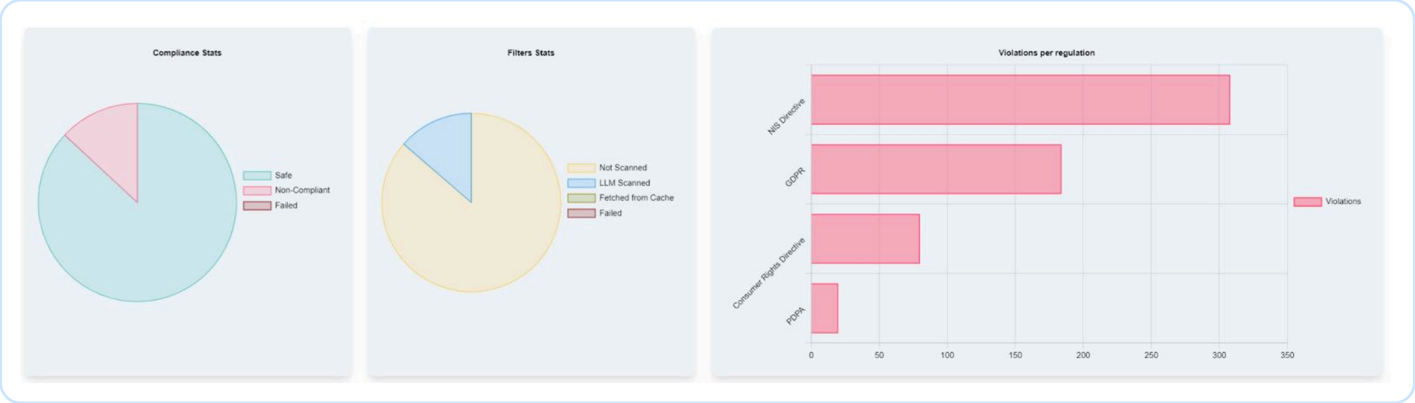
The inclusion of an API key in the email could potentially expose sensitive information and increase the risk of unauthorized access to the organization's systems or data, which could violate the NIS Directive and GDPR regulations., Confidence is High because: The inclusion of an API key in an email is a clear security risk that could lead to unauthorized access and data breaches., Severity is Moderate because: The exposure of an API key could potentially lead to a data breach, but the extent of the harm would depend on the specific data and systems accessed through the API.

For instance, the system can spot when personal medical records are shared in an email, which would violate both HIPAA and GDPR.

Action recommendations

When GFI Archiver AI identifies violations, it creates tailored recommendations for each issue. These may include:

- **Password Reset:** Require a password change for all affected accounts to prevent unauthorized access.
- **Notification:** Inform affected individuals about the breach and give them clear steps to protect themselves.
- **Redaction:** Remove or hide sensitive information to protect privacy.
- **Security Review:** Investigate how the breach happened and implement measures to prevent future incidents.
- **Data Protection:** Add more security measures, such as encryption and tighter access controls.
- **Compliance Reporting:** Report the breach to the necessary regulatory bodies, as required by law.
- **Training:** Provide employees with training on secure communication and best practices to prevent similar incidents in the future.
- **Documentation:** Keep detailed records of the incident and the steps taken to address it for compliance and auditing.
- **Policy Updates:** Review and update relevant policies and procedures to help prevent similar incidents.



GFI Archiver AI makes archiving easier and reduces the workload for administrators and compliance officers. It understands relevant regulations, scans emails for violations, and creates easy-to-read compliance reports. This helps your organization effortlessly handle data compliance and self-assessment.