newgen

Think Outside the Inbox

Modernising Email Archival & Records Management

for the Next Era of Governance

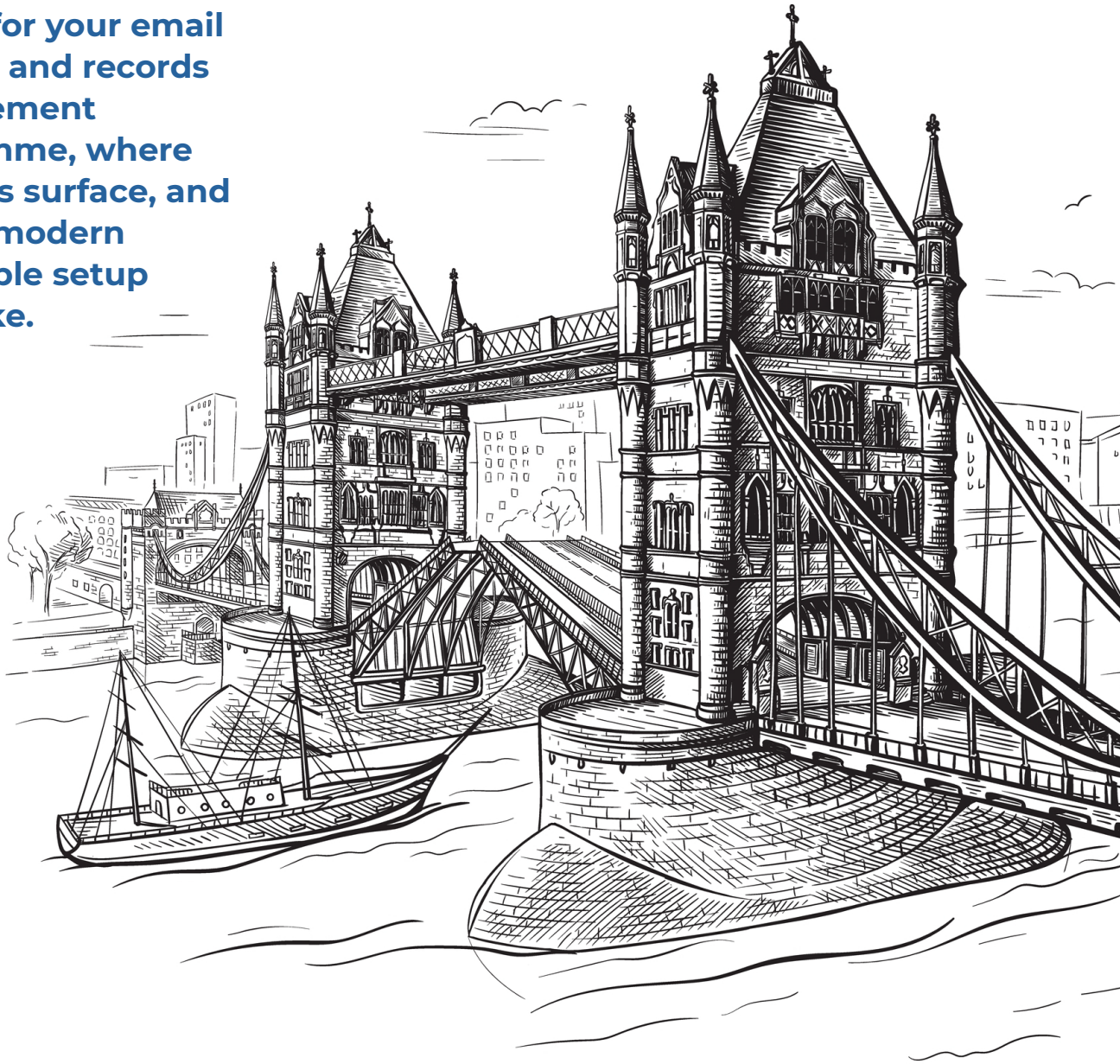
Demonstrating Control When UK & Europe Regulators Stop Writing Rules

Overview

In the UK and across Europe, the standard for governing business communications is changing shape. For years, compliance meant following the rule, i.e., read the handbook, apply the requirement, file the policy. It no longer holds the way it once did before. The Financial Conduct Authority had stepped back from writing a rule for every scenario. The authority now examines whether a firm can show its controls work in practice.

Addressing it sounds harder today because two bodies of law seem to be pushing you in different directions. European recordkeeping law tells you to keep a great deal of records, for years, unaltered. Data protection law asks you to keep as little as you can justify, and to erase on request. Not all firms can, with confidence, claim they are doing both well.

This whitepaper addresses the dilemma, what it means for your email archival and records management programme, where the gaps surface, and what a modern defensible setup looks like.



The Breach that Trickles from the Top

Every enterprise has a records/communication policy that clearly defines exactly which channels teams may use for business. It stands reviewed by legal and approved by senior management. By any reasonable measure, it is sound.

Looks fine on paper. However, the data points otherwise.

In August 2025, the FCA published findings from a review of off-channel communications across eleven wholesale banks, framed as a state-of-play assessment. The regulator counted 178 breaches of internal communications policies in a single year. Of those, a **large share came from the most senior people in the building.**

The instinct, facing a behavioural problem, is to write a firmer rule. The FCA has chosen not to. In early 2025 its chief executive said the regulator does not intend to write a new rule for every communication scenario/challenge.

So, the question being asked of you has shifted. The conversation now steers to whether you can prove archival and records management works, detect when it does not, and show the same standard reaches the top.

There is a sharper edge coming too. From 1 September 2026, the FCA's non-financial misconduct rules extend across the Senior Managers and Certification Regime, bringing serious conduct into scope even when it travels through unmonitored channels. The surface area your governance must cover is widening, and **email is where the gap between stated policy and real behaviour shows first.**

41%

of off-channel policy breaches involved individuals at director grade or above.

Source: FCA, August 2025

Three Things Supervision Now Tests

Read the August review alongside the FCA's SYSC recordkeeping principles and the ICO's guidance on retention, and the expectations can be broadly settled into three areas.

These are the places where the divide between what a firm says and what it does becomes visible, and where that distance carries the most weight. The tricky part is that a firm can be strong on one and exposed on the other two.

#1 Control

A policy stating that staff must use approved channels is a statement of intent. Evidence that you capture communications across those channels, apply retention consistently, and can produce the records on request is something else.

Genuine control has to run continuously and automatically. The firms that came through the review well had built control into their systems, so that capture and retention happened by default.

#2 Breaches

You cannot manage what you cannot see, and off-channel communication is the activity designed to be invisible. This weighs whether firms could detect breaches of their own policies, and how good is the management information surfacing them.

Detection is where many programmes struggle. A firm can run a clean archive for the channels it monitors while having no way to know when business slipped.

#3 Accountability

Under the UK regime, reinforced by the Senior Managers and Certification Regime, governance failures are treated as questions of management responsibility. The expectation is whether senior leaders set the tone, understood their own obligations, and whether the culture beneath them matched the policy.

The hard part is that the people who most need to model the behaviour often have the most autonomy and the least appetite for friction. Accountability that reaches the top shows up as evidence that the same control and the same consequences apply to the executive committee as to everyone else. Where that evidence exists, the culture story tells itself.

Dual Obligations of the Same Mailbox

A firm operating across the UK and Europe sits between two requirements that, read quickly, look like they collide. One sets a floor under **what must be retained.** The other sets limits on **what may be kept.** The same mailbox answers to both.

1. **The retention floor.** MiFID II, which the UK retained after Brexit, requires firms to record communications relating to client orders or that could lead to a transaction, across every channel, including personal devices and messaging apps. Those records stay for at least five years, extendable to seven on an authority's request, stored so they cannot be altered, with every change traceable. The FCA gives these obligations effect in its handbook through SYSC 10A.
2. **The privacy limits.** The UK GDPR and the EU GDPR require personal data to be kept no longer than necessary, give individuals a right to erasure, and warn against holding data, in the ICO's phrase, on the off chance it might be useful.

The MiFID II Retention Floor	The UK & EU GDPR Privacy Limits
Retain relevant communications for at least 5 years	Keep personal data no longer than necessary for its purpose
Extend to seven years when an authority requests it	Honour a right to erasure on request
Store tamper-proof, with every change traceable	Avoid keeping data on the off chance it proves useful
Capture every channel, including personal devices	Apply purpose limitation and data minimisation

Read side by side, the two look like a standoff. In law, they are not.

The right to erasure is not absolute. Where retention is necessary to meet a legal obligation, and a regulatory requirement, the erasure right falls away. So, where MiFID II requires a record to be kept, an erasure request does not override it. Where no such duty exists, the record should be removed once its purpose ends.

The whole thing becomes an operational challenge. The hard part is telling, across a high-volume mailbox, which records sit under a retention duty, and which carry none. **When a firm can classify each communication, apply the right retention rule to the right record, and remove personal data once no obligation requires keeping it, the apparent collision disappears.** MiFID-scope records are kept, tamper-proof, for the full term. Personal data with no retention duty is erased on request. The difference is precision in classification.

What a Defensible Setup Requires

The 3 areas look like separate problems. **Control, detection, accountability.** Reverse-engineer what it takes to hold all three, and you land on the same six capabilities every time.

Capture creates the record. Classification decides where it lands. Surveillance watches for the gaps. Integrity makes every action provable. Retention and erasure fulfil both requirements. Retrieval extracts the whole chain when it matters.

Think of them as the working parts of **one orchestrated system,** where what you keep, what you remove, and who is accountable for either can be produced on demand.

Capability	How it Works	Solves for
Capture	Ingests business communications at the point they are sent or received, with full metadata and attachments, so nothing depends on personal mailboxes.	**#1 Control and #3 Accountability**
Classification	Sorts each communication by record type and applies the correct retention rule, so MiFID II records are kept, and personal data is not held past its purpose.	**#1 Control**
Surveillance	Surfaces policy breaches and signals when business drifts toward unmonitored channels, turning management information into something supervision recognises.	**#2 Breach**
Integrity	Preserves records tamper-proof, with full audit logs of access, change, and export, so the accountability trail exists without anyone assembling it by hand.	**#3 Accountability**
Retention & Erasure	Enforces retention and executes lawful erasure from one controlled process, satisfying both climates through the same evidenced workflow.	**#1 Control**
Retrieval	Produces records on demand, with full context and provenance, so the firm can answer a regulator or an investigation within the timeframes expected.	**#2 Breach**

Building Toward the Proof

The setup also answers five questions any serious email records programme should be ready for. The auditor won't ask you categorically. It's a mental model to keep in place while building towards a fool-proof system.

- Can you show complete capture for any person and period?
- Can you produce records quickly?
- Can you prove nothing was altered?
- Can you explain why you kept what you kept and removed what you removed?
- Can you show the scope of any hold?

A Phased Path

Here's a phased approach framed around evidence. Three phases, each named for its outcome.

1 Phase

Diagnostic Certainty

- Map every channel where business communication happens, monitored and unmonitored
- Identify where activity drifts off-channel, and where the senior-grade risk concentrates
- Locate current records and retention practice, and test whether control is real or merely stated
- Document the dual obligations that apply, from SYSC 10A and MiFID II to the GDPR

Deliverable: An honest picture of where communication lives, where control is genuine, and where the gaps sit.

2 Phase

Control Proof

- Establish automatic capture across approved channels, removing reliance on individual diligence
- Build classification that applies the right retention rule to the right record
- Put integrity controls and audit logging in place, aligned with MiFID II tamper-proofing
- Run a dual test, satisfying a records request and an erasure obligation in the same exercise

Deliverable: A working pilot that produces evidence as routine rather than reconstructing it under pressure.

3 Phase

Supervision Readiness

- Run a realistic production exercise and confirm records can be produced at speed
- Trace how a simulated off-channel drift would be surfaced and recorded
- Confirm the same controls and consequences demonstrably reach the most senior grades
- Establish the routines that keep control, detection, and accountability current over time

Deliverable: Evidence that the three areas hold under realistic conditions, with routines that keep them holding.

Orchestrating It All with Newgen

Everything in this whitepaper describes what a defensible communications governance programme in the UK and Europe needs to do. The three areas supervision tests, the architecture that makes them operational, and the phased path to proof. Making it work takes more than a set of tools. **It takes a platform that orchestrates the parts as one governed system.**

Our **NewgenONE Contextual Content Services (ECM) platform** brings structure and control to enterprise email through intelligent archiving, lifecycle-driven records management, and consistent governance at scale. Business records and communications are captured at the source, preserved in a tamper-resistant repository, and indexed for retrieval under supervisory conditions. Retention rules are embedded and applied automatically, so control operates by default. Lawful erasure runs as a controlled, evidenced event. Access is logged, and accountability is traceable to the individual.

ONE ORCHESTRATED SYSTEM

Capture → Classification → Surveillance → Integrity → Retention & Erasure → Retrieval

NewgenONE Contextual Content Services (ECM)
One governed, orchestrated layer

Within that system, each capability does a distinct job.

Capture
Policy-based ingestion across email and messaging channels with full metadata and attachment preservation, independent of personal mailboxes.

Classification
AI-assisted categorisation tied to consistent retention rules and sensitivity levels, turning policy into automated enforcement.

Surveillance
Monitoring and management information that surfaces policy breaches and supports the detection the FCA expects firms to demonstrate.

Integrity
Tamper-resistant archiving with comprehensive audit trails and access logging, aligned with MiFID II expectations on traceability.

Retention & Erasure
Automated retention enforcement and lawful erasure from one documented workflow, satisfying both obligations.

Retrieval
Fast search, filtering, and export across bodies, metadata, and attachments, designed for supervisory and eDiscovery demands.

For more than three decades, across 76 countries, enterprises have trusted Newgen as their digital transformation partner to orchestrate intelligent enterprises at scale.

Are Your Systems Modern?

See where your email records governance stands in a 30-minute session with our team. We will help you find where control, detection, and accountability are strongest, and where the gaps live.

About Newgen

Newgen Software Orchestrates Intelligent Enterprises at scale. The NewgenONE Platform unifies content, processes, and communications into an orchestration layer where intelligence is embedded into how enterprises operate, with trust, governance, and control built in. Enterprises move beyond fragmented initiatives to continuously adaptive, production-ready operations. Decisions, workflows, and experiences evolve in real time, shaped by context, data, and embedded AI. Trusted by leading organizations worldwide, Newgen defines how modern enterprises operate, intelligently and at scale.

For Sales Query

AMERICAS: +1 (202) 800 77 83

CANADA: +1 (202) 800 77 83

AUSTRALIA: +61 290 537174

INDIA: +91 11 407 73769

APAC: +65 3157 6189

MEA: +971 600 521 468, +27 11 461 6497

EUROPE: +44 (0) 2036 514805

info@newgensoft.com

www.newgensoft.com

newgen