

FREE RESOURCE — COMPLIANCE CHECKLIST

Email Archiving & Compliance Checklist

Validate your email archiving setup against UK GDPR, HMRC and Companies Act retention, eDiscovery and legal hold obligations. Score each of four compliance areas to surface gaps before a regulator, an auditor or a litigation request finds them first.

4

COMPLIANCE
AREAS
COVERED

27

CHECKLIST
ITEMS
TO VERIFY

/10

SCORE EACH
SECTION

Fillable

TICK & TYPE
IN ANY VIEWER

UK GDPR

HMRC RETENTION

LEGAL HOLD

EDISCOVERY

PREPARED FOR

Cloudswitched Knowledge
Library

PREPARED BY

Cloudswitched Ltd.

EDITION

2026 · UK GDPR

FORMAT

Interactive PDF

00

How to use this checklist

Work through each of the four sections with your compliance officer, legal counsel and IT lead. Tick every checkpoint that is **fully in place** today — with evidence: a written policy, a configuration screenshot, a DPIA, a journal report, a successful test export. Half measures do not tick.

Email archiving must satisfy several overlapping regimes at once — UK GDPR data minimisation, HMRC and Companies Act retention, FCA record-keeping (where applicable), litigation hold, and eDiscovery. Where the rules conflict, the more specific legal retention obligation generally prevails over the GDPR minimisation principle — provided the legal basis is documented.

WHAT THIS CHECKLIST IS

A baseline self-assessment for UK SMEs covering the four compliance areas every email archive must address: retention policy, UK GDPR, technical implementation, and legal hold & eDiscovery. It is not a substitute for legal advice on a specific matter, and it does not certify any standard, but it surfaces the gaps that regulators, auditors and opposing counsel will find first.

SCORING GUIDANCE

Award one or two points per checkpoint where you have hard evidence the control is in place — a policy document, a journaling configuration, a test restore log, a DPIA, a legal hold runbook. Round each section to the nearest whole number out of 10 and carry it forward to the summary on page 7. Anything below 6 is a candidate for the top-3 priority actions.

The four sections

- **01 Retention Policy Framework** — documented policy, category-specific periods, HMRC/Companies Act alignment, legal counsel sign-off.
- **02 UK GDPR Compliance** — personal data identification, DSARs, right to erasure, lawful basis, RoPA entry, encryption, DPIA.
- **03 Technical Implementation** — archiving solution, WORM/tamper-proof storage, full-text search, journaling, independent backup, export formats.
- **04 Legal Hold & eDiscovery** — documented hold process, deletion override, search filters, secure export, chain of custody, custodian-level scope.

01

Retention Policy Framework

Establish clear email retention periods aligned with UK statutory obligations — HMRC, Companies Act 2006, Limitation Act 1980 — and document the legal basis for each. An undocumented retention policy is the single biggest source of audit findings in this domain.

- ☐ A **documented email retention policy** exists and has been formally approved by senior management.
- ☐ **Retention periods** are defined for each email category — general correspondence, financial, HR, legal, client.
- ☐ **Financial emails** are retained for a minimum of 7 years (*Companies Act 2006, HMRC record-keeping*).
- ☐ **HR-related emails** are retained for a minimum of 6 years after employment ends (*Limitation Act 1980*).
- ☐ **Contract-related emails** are retained for 6 years after contract completion (*12 years for contracts executed as deeds*).
- ☐ A process exists to **delete emails** that have exceeded their retention period — the archive is not retained indefinitely.
- ☐ The retention policy has been **reviewed by legal counsel** for UK regulatory compliance.

POLICY METADATA TO RECORD

Capture the live policy version, retention period and DPO contact on the sign-off page so any reviewer can verify the authoritative source.

SECTION 01 SCORE / 10

Aim for 8+. Below 6 = retention policy gap.

02

UK GDPR Compliance

Ensure email archiving practices comply with UK GDPR data protection requirements — lawful basis, DSAR fulfilment, right to erasure where retention allows, encryption, and a current Data Protection Impact Assessment for the archive itself.

- ☐ Email containing **personal data** is identified and managed in accordance with your privacy notice.
- ☐ **Data Subject Access Requests (DSARs)** can be fulfilled from the email archive within the 30-day statutory window.
- ☐ The **right to erasure** can be applied to email archives where no overriding legal basis for retention exists.
- ☐ A **lawful basis** for retaining email data is documented — legitimate interest, legal obligation, contract, or consent.
- ☐ **Data processing records (RoPA)** include email archiving as a processing activity with purpose and retention stated.
- ☐ Email archives are **encrypted** at rest and in transit, with access restricted to authorised personnel.
- ☐ A **Data Protection Impact Assessment (DPIA)** has been conducted for email archiving.

GDPR VS LEGAL RETENTION

GDPR requires data minimisation — do not keep data longer than necessary. Other laws require retention (e.g. 7 years for financial records). Document the legal basis for each retention period. Where GDPR and retention obligations conflict, the specific legal retention requirement generally takes precedence.

SECTION 02 SCORE / 10

Aim for 9+. Below 6 = data protection risk.

03

Technical Implementation

Verify the technical setup of email archiving meets compliance and recovery requirements — tamper-proof storage, full-text search, journaling, independent backup, and supported export formats for legal discovery.

- ☐ An **email archiving solution** is in place (*M365 retention policies, Mimecast, Barracuda or equivalent*).
- ☐ Archived emails are stored **tamper-proof** — WORM (Write Once Read Many) for regulatory compliance.
- ☐ The archive supports **full-text search** across sender, recipient, subject, body and attachments.
- ☐ **Journaling** is configured to capture all email (including deleted messages) in the archive.
- ☐ Archive storage is **separate from primary email** — not relying solely on user mailbox retention.
- ☐ Archive **data is backed up** independently with its own backup and retention policy.
- ☐ The archive can export data in **standard formats** (PST, EML) for legal discovery or regulatory requests.

M365 RETENTION IS NOT A BACKUP

Microsoft 365 retention policies cover regulatory retention only. They do not protect against ransomware-encrypted mailboxes, malicious admin deletion, or tenant lockout. Independent third-party archive backup is a separate control — check the next line in the list.

SECTION 03 SCORE ----- / 10

Aim for 8+. Below 6 = archive integrity gap.

04

Legal Hold & eDiscovery

Confirm you can place a legal hold and respond to discovery requests within commercially reasonable time. The first time you test your legal hold process should not be when opposing counsel has just put your firm on notice.

- ☐ A **legal hold process** is documented and can be activated within 24 hours of notification.
- ☐ Legal holds **override deletion policies** to preserve all relevant email during litigation or investigation.
- ☐ The archive supports **eDiscovery search** with date range, keyword, sender/recipient and attachment filters.
- ☐ eDiscovery results can be **exported and shared** securely with legal counsel.
- ☐ **Chain of custody** is maintained for all email evidence produced for legal proceedings.
- ☐ Legal holds can be applied to **specific custodians** without affecting other users.

TEST BEFORE YOU NEED IT

Schedule an annual tabletop exercise: pretend a litigation hold notice has just arrived for two named custodians and four search terms over a 24-month window. Time how long it takes from notice to first export. Anything over a day in a known-good case is a process problem you want to find on a Tuesday, not in court.

SECTION 04 SCORE / 10

Aim for 8+. Below 6 = litigation exposure.



Compliance score summary

Transfer the score for each section into the table. Set a priority (H/M/L) based on the gap to target. Anything below 6 is a candidate for the top-3 actions on the next page.

#	COMPLIANCE AREA	SCORE / 10	PRIORITY
01	Retention Policy Framework	_____ / 10	☐ H ☐ M ☐ L
02	UK GDPR Compliance	_____ / 10	☐ H ☐ M ☐ L
03	Technical Implementation	_____ / 10	☐ H ☐ M ☐ L
04	Legal Hold & eDiscovery	_____ / 10	☐ H ☐ M ☐ L
Σ	TOTAL SCORE	_____ / 40	—

Policy metadata — the live source of truth

Record the authoritative values that govern your archive. Any reviewer who needs to challenge a retention decision should be able to find them here.

POLICY VERSION

EFFECTIVE FROM

DEFAULT RETENTION PERIOD

DPO / DATA PROTECTION LEAD

DPO CONTACT EMAIL

ARCHIVE SOLUTION



Interpretation, actions & sign-off

Translate your total score into a risk band, capture the top three priority actions, and have the compliance owner sign the bottom of the page. Anything below 24/40 needs a remediation plan with named owners.

Score interpretation (out of 40)

32–40

Excellent. Your archive is well-managed against UK retention, GDPR and litigation obligations. Focus on annual review and tabletop exercises.

24–31

Good foundation, gaps exist. Prioritise any area scoring below 6 with owners and deadlines. Re-test legal hold within 90 days.

Below 24

Significant gaps. Material exposure to regulator action, GDPR enforcement and litigation cost. Seek specialist review.

Top 3 priority actions

01

02

03

Compliance sign-off

REVIEWED BY (NAME)

ROLE / TITLE

SIGNED ON

SIGNATURE

NEXT REVIEW DUE

Need email archiving set up properly?

Cloudswitched implements compliant email archiving for UK SMEs on Microsoft 365 — retention policies, journaling, WORM storage, legal hold and eDiscovery, with documented DPIA and RoPA evidence.

info@cloudswitched.com

cloudswitched.com/solutions/cloud-email



CLOUDSWITCHED

EMAIL ARCHIVING & COMPLIANCE

info@cloudswitched.com

New London House, 6 London St
London EC3R 7LP · United Kingdom