Email Archiving & Compliance Checklist

Email retention policies meeting UK GDPR, regulatory requirements, and legal hold obligations. Ensure your email archiving strategy protects your organisation.

6	7yr	72hr	Free
COMPLIANCE AREAS	TYPICAL FINANCIAL RETENTION	BREACH NOTIFICATION DEADLINE	COMPLIANCE CHECKLIST

How to Use This Checklist

Review each section with your compliance officer, legal advisor, and IT team. Email archiving must satisfy multiple overlapping requirements: legal, regulatory, GDPR, and business. Tick items that are fully in place and create an action plan for gaps.

1 Retention Policy Framework

Establish clear email retention policies aligned with legal and regulatory requirements.

- [ ] A **documented email retention policy** exists and has been approved by senior management
- [ ] Retention periods are defined for each **email category**: general correspondence, financial, HR, legal, client
- [ ] **Financial emails** are retained for minimum 7 years (Companies Act 2006, HMRC requirements)
- [ ] **HR-related emails** are retained for minimum 6 years after employment ends (Limitation Act 1980)
- [ ] **Contract-related emails** are retained for 6 years after contract completion (12 years for deeds)
- [ ] A process exists to **delete emails** that have exceeded their retention period (do not retain indefinitely)
- [ ] The retention policy has been **reviewed by legal counsel** for UK regulatory compliance

Section Score: _____/10

2 UK GDPR Compliance

Ensure email archiving practices comply with UK GDPR data protection requirements.

- [ ] 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 30 days
- [ ] 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, consent)
- [ ] **Data processing records** 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

Section Score: ____/10

GDPR vs Legal Retention

GDPR requires data minimisation (do not keep data longer than necessary), but 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.

3 Technical Implementation

Verify the technical setup of email archiving meets compliance and recovery requirements.

- [ ] 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

Section Score: ____ /10

4 Legal Hold & eDiscovery

Ensure you can place legal holds and respond to discovery requests.

- [ ] 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

Section Score: ____ /10

#	AREA	SCORE	PRIORITY
1	Retention Policy Framework	/ 10	H / M / L
2	UK GDPR Compliance	/ 10	H / M / L
3	Technical Implementation	/ 10	H / M / L
4	Legal Hold & eDiscovery	/ 10	H / M / L
TOTAL SCORE		**/ 40**	

Score Interpretation

80–100: Excellent — well-managed with only minor improvements needed.
60–79: Good foundation but gaps exist. Prioritise areas scoring below 6.
Below 60: Significant gaps putting your business at risk. Seek specialist review.

! Action Items & Notes

Top 3 Priority Actions:

1. _____
2. _____
3. _____

Notes

_____

Completed By: _____ Date: _____ Next Review: _____