Backup Retention Policy Guide

Retention schedules based on legal, regulatory, and business requirements. Define how long to keep backups for every data category in your organisation.

7yr	6yr	GDPR	Free
FINANCIAL DATA RETENTION	EMPLOYMENT RECORDS	DATA MINIMISATION PRINCIPLE	RETENTION GUIDE

1 UK Regulatory Retention Requirements

Understand the legal and regulatory frameworks that determine minimum retention periods for UK businesses.

REGULATION / LAW	DATA TYPE	MINIMUM RETENTION	AUTHORITY
Companies Act 2006	Financial records, accounts	6 years from end of financial year	Companies House
HMRC requirements	Tax records, VAT, PAYE	6–7 years	HMRC
Limitation Act 1980	Contract records	6 years (12 for deeds)	Courts
Employment Rights Act 1996	Employee records	6 years after leaving	Employment Tribunal
Working Time Regulations	Working hours records	2 years	HSE
Health & Safety	Accident records	3 years (40 years for COSHH)	HSE
UK GDPR	Personal data	No longer than necessary	ICO

GDPR Tension

UK GDPR requires you to delete personal data when it is no longer needed (data minimisation). However, other laws require you to retain certain records for specific periods. Document the legal basis for each retention period. When the legal retention period expires, the data should be securely deleted.

2 Recommended Retention Schedule

DATA CATEGORY	BACKUP RETENTION	LEGAL BASIS	DELETE AFTER
Financial records & accounts	7 years	Companies Act, HMRC	7 years from financial year end
Employee HR records	6 years after leaving	Limitation Act	6 years after employment ends
Payroll & PAYE records	7 years	HMRC	7 years from end of tax year
Customer contracts	6 years after completion	Limitation Act	6 years after contract ends
Client correspondence	3 years	Business need	3 years after last contact
Marketing & consent records	Duration + 2 years	UK GDPR	2 years after consent withdrawn
IT system logs	1 year	Security best practice	12 months rolling
CCTV footage	30 days	ICO guidance	30 days unless incident
Board minutes	Permanently	Companies Act	Do not delete
Insurance records	Duration + 6 years	Limitation Act	6 years after policy ends

3 Backup Retention Tiers

Apply a tiered retention approach to balance storage costs with recovery needs.

TIER	BACKUP TYPE	FREQUENCY	RETENTION PERIOD		
Tier 1	Continuous / Real-time	Continuous	24–72 hours	Local / SSD	Highest
Tier 2	Daily incremental	Every 24 hours	30 days	Cloud (hot storage)	Medium
Tier 3	Weekly full	Every 7 days	12 weeks	Cloud (cool storage)	Lower
Tier 4	Monthly archive	Monthly	12 months	Cloud (cool storage)	Lower
Tier 5	Annual archive	Annual	7 years	Cloud (archive storage)	Lowest

Storage Cost Optimisation

Use cloud storage tiers to optimise costs. Recent backups (Tier 1–2) should be on fast, accessible storage for quick recovery. Older archives (Tier 4–5) can use cold/archive storage at significantly lower cost. Azure Archive Storage costs as little as £0.001/GB/month.

4 Secure Disposal Procedures

When retention periods expire, data must be securely and verifiably destroyed.

- → **Digital data:** Use certified data destruction software that overwrites data and provides a destruction certificate. For cloud backups, verify the provider's deletion process meets your requirements.
- → **Physical media:** Hard drives, tapes, and USB devices must be physically destroyed (shredded) by a certified WEEE contractor. Obtain destruction certificates with serial numbers.
- → **Paper records:** Use cross-cut shredding (minimum DIN 66399 Level P-4 for confidential data). For large volumes, use a certified confidential waste contractor.
- → **Record keeping:** Maintain a destruction log recording what was destroyed, when, by whom, and the destruction method. Retain destruction records for 7 years.

Notes