Data Retention Policy

Company Name: Compitel

Effective Date: 10th November 2025

Review Date: 10th November 2026

Version: 1.0

1. Purpose

This policy outlines Compitel's approach to retaining, archiving, and securely disposing of personal and healthcare-related data in compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and NHS Digital guidelines.

2. Scope

This policy applies to all personal data processed by Compitel in the course of providing IT services to healthcare providers. It covers data stored in electronic and physical formats, including backups and audit logs.

3. Principles

We adhere to the following principles regarding data retention:

- **Data Minimisation**: Only retain data necessary for the intended purpose.
- **Storage Limitation**: Do not keep personal data longer than necessary.
- **Security**: Ensure secure storage and disposal of data.
- **Accountability**: Maintain records of retention periods and disposal actions.

4. Retention Periods

Data Type	Retention Period	Justification
Patient health records (processed on behalf of clients)	As per client instructions or NHS Records Management Code of Practice	Legal and contractual obligation
System access logs and audit trails	8 years	NHS DSP Toolkit and audit requirements
Support tickets and service logs	6 years	Business and legal reference
Employee records	6 years after termination	Employment law compliance
Financial records (invoices, contracts)	7 years	HMRC requirements
Email correspondence (non-clinical)	3 years	Operational reference
Backup data	30–90 days (rolling)	Business continuity and disaster recovery

Note: Where retention periods are defined by the client (e.g., NHS Trusts), those take precedence.

5. Data Disposal

At the end of the retention period, data is securely disposed of using the following methods:

- **Electronic data**: Secure deletion using certified data erasure tools
- **Physical records**: Shredding or incineration by approved vendors
- **Backups**: Overwritten or destroyed in accordance with backup lifecycle policies

6. Roles and Responsibilities

Role	Responsibility
Data Protection Officer (DPO)	Oversees compliance with retention schedules
IT & Security Team	Implements secure deletion and backup rotation
Department Heads	Ensure operational data is reviewed and archived appropriately

7. Exceptions

In certain cases, data may be retained longer if:

- Required by law or regulation
- Necessary for legal proceedings or investigations
- Explicitly requested by the client under contract

8. Monitoring and Review

This policy is reviewed annually or upon significant changes in legislation, client requirements, or business operations.