Data Protection Policy

For: Compitel

Effective Date: 10th November 2025

Review Date: 10th November 2026

1. Purpose

This policy outlines how Compitel protects personal data, particularly sensitive health information, in compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and applicable NHS data security standards.

2. Scope

This policy applies to all employees, contractors, and third parties who access or process personal data on behalf of Compitel, including data processed on behalf of healthcare clients.

3. Definitions

- **Personal Data**: Any information relating to an identified or identifiable individual.
- **Special Category Data**: Includes health data, genetic and biometric data.
- **Data Subject**: The individual whose data is being processed.
- **Data Controller**: The entity that determines the purposes and means of processing personal data.
- **Data Processor**: The entity that processes data on behalf of the controller.

4. Legal Basis for Processing

We process healthcare data under the following lawful bases:

- **Article 6(1)(b)**: Processing necessary for the performance of a contract.
- **Article 6(1)(c)**: Compliance with a legal obligation.
- **Article 9(2)(h)**: Processing necessary for the provision of health or social care.

5. Data Protection Principles

We adhere to the following principles:

- **Lawfulness, fairness, and transparency**
- **Purpose limitation**

- **Data minimisation**
- **Accuracy**
- **Storage limitation**
- **Integrity and confidentiality**
- **Accountability**

6. Data Subject Rights

We uphold the rights of data subjects, including:

- Right to access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights related to automated decision-making

7. Data Security Measures

We implement appropriate technical and organisational measures, including:

- Encryption of data at rest and in transit
- Role-based access controls
- Regular penetration testing and vulnerability assessments
- Secure coding practices
- Staff training on data protection and cyber hygiene
- Incident response and breach notification procedures

8. Data Sharing and Transfers

- Data is only shared with authorised third parties under strict contractual controls (e.g., Data Processing Agreements).
- International data transfers are conducted in compliance with UK GDPR (e.g., using Standard Contractual Clauses).

9. Data Retention

- Data is retained only as long as necessary for the purpose it was collected.

- Retention schedules are defined in our Data Retention Policy.

10. Data Breach Management

- All breaches are reported to the Data Protection Officer (DPO) immediately.
- Serious breaches are reported to the ICO within 72 hours.
- Affected data subjects are notified when required.

11. Roles and Responsibilities

Role	Responsibility
Data Protection Officer (DPO)	Oversees compliance and acts as point of contact
All Staff	Must comply with this policy and report incidents

12. Training and Awareness

- Mandatory data protection training for all staff
- Annual refresher courses and updates

13. Monitoring and Review

- This policy is reviewed annually or upon significant legal/operational changes