

FELIKOT

Data Protection Policy

Effective Date: May 2023

Next Review Date: May2026

Approved by: Information Governance Board

1. Purpose	2
2. Scope	2
3. Definitions	2
4. Data Protection Principles	2
5. Lawful Basis for Processing	2
6. Individual Rights	2
7. Data Security	3
8. Data Breaches	3
9. Data Sharing and Transfers	3
10. Retention and Disposal	3
11. Training and Awareness	3
12. Policy Review	4

1. Purpose

This Data Protection Policy outlines how **Felikot Healthcare Ltd** collects, processes, stores, and protects personal data in compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and any other applicable data protection legislation.

2. Scope

This policy applies to all employees, contractors, consultants, partners, and third parties who access or process personal data on behalf of Felikot Healthcare Ltd.

3. Definitions

- **Personal Data:** Any information relating to an identified or identifiable individual.
- **Special Category Data:** Sensitive personal data including race, religion, health information, etc.
- **Processing:** Any operation performed on personal data (e.g., collection, storage, access, disclosure).
- **Data Subject:** The individual whose data is being processed.
- **Data Controller:** Felikot Healthcare Ltd, who determines how and why personal data is processed.
- **Data Processor:** Any third party who processes personal data on behalf of Felikot Healthcare Ltd.

4. Data Protection Principles

Felikot Healthcare Ltd is committed to ensuring that personal data is:

1. **Processed lawfully, fairly and transparently**
2. **Collected for specified, explicit and legitimate purposes**
3. **Adequate, relevant and limited to what is necessary**
4. **Accurate and kept up to date**
5. **Kept only as long as necessary**
6. **Processed securely**

5. Lawful Basis for Processing

Felikot Healthcare Ltd will only process personal data where there is a lawful basis, including:

- Consent from the individual
- Performance of a contract
- Compliance with a legal obligation
- Protection of vital interests
- Legitimate interests pursued by Felikot Healthcare Ltd or a third party (balanced with the rights of the individual)

6. Individual Rights

Felikot Healthcare Ltd recognises and upholds the following rights of data subjects:

- Right to be informed

- Right of access
- Right to rectification
- Right to erasure (“right to be forgotten”)
- Right to restrict processing
- Right to data portability
- Right to object
- Rights in relation to automated decision-making and profiling

Requests to exercise these rights should be submitted to:

Email: [insert email, e.g., dataprotection@felikothhealthcare.com]

Data Protection Officer (DPO): [insert name if applicable]

7. Data Security

Felikot Healthcare Ltd will implement appropriate technical and organisational measures to protect personal data including:

- Encryption and pseudonymisation
- Access controls and authentication
- Secure storage (physical and digital)
- Staff training on data protection
- Regular audits and risk assessments

8. Data Breaches

In the event of a data breach, Felikot Healthcare Ltd will:

- Investigate and contain the breach
- Assess the risk to individuals
- Notify the ICO within 72 hours if required
- Inform affected individuals when necessary

All incidents must be reported immediately to the DPO or relevant line manager.

9. Data Sharing and Transfers

- Personal data will not be shared with third parties unless there is a legal basis or data processing agreement in place.
- Any international data transfers outside the UK/EU will be conducted in compliance with relevant adequacy decisions or safeguard mechanisms (e.g., Standard Contractual Clauses).

10. Retention and Disposal

Felikot Healthcare Ltd retains personal data only for as long as necessary for the purposes it was collected. Once no longer needed, data will be securely deleted or anonymised in line with the Data Retention Policy.

10.1 Data Retention Schedule

Category of Data	Description / Examples	Retention Period	Legal Basis / Notes
Employee Records	Contracts, disciplinary records, payroll, training	6 years after termination	Limitation Act 1980 – for defending employment claims
Job Application Data	CVs, application forms	2 months	ICO guidance – unless extended with consent for future opportunities
Health and Safety Records	Accident reports, risk assessments	3 years (adults) / Until child is 21 (for minors)	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (RIDDOR)
Patient Health Records (Adults)	Medical history, diagnosis, treatment notes	8 years after last treatment	NHS Records Management Code of Practice for Health and Social Care
Patient Health Records (Children)	Medical records of minors	Until 25th birthday (or 26 if treated at 17)	NHS Records Management Code of Practice
CCTV Footage (if applicable)	Video surveillance	30 days (standard)	Unless needed for investigation or legal proceedings
Client/Customer Data	Contact details, correspondence, billing	6 years after last interaction	Limitation Act – for contract claims or legal disputes
Financial and Tax Records	Invoices, receipts, VAT records, bank statements	6 years	HMRC requirement
Consent Forms	Patient or research participant consent forms	8 years	NHS guidance – or longer if part of medical record
Marketing Contact Information	Email addresses, opt-in records	Until withdrawal of consent / 2 years inactive	Consent required under PECR and UK GDPR
Subject Access Request Records	Correspondence, identity verification	3 years	ICO guidance – for audit and complaint handling

Retention Notes

- Data will be securely destroyed or anonymised at the end of its retention period.
- Retention may be extended where legal proceedings are anticipated or ongoing.
- All electronic and physical data will be reviewed regularly for compliance.

11. Training and Awareness

All staff will receive regular data protection training and are required to follow this policy. Failure to do so may result in disciplinary action.

12. Policy Review

This policy will be reviewed annually or in response to changes in legislation, business practices, or data protection risks.

Document Control

- **Owner:** Data Protection Officer
- **Version:** 2.1
- **Approved by:** Information Governance Board
- **Last Updated:** May 2025