Data Protection Policy

Document Control

Document Owner: CEO

Approval Date: 18/08/2025
Effective Date: 18/08/2025
Review Date: August 2026

Note: This policy must be reviewed annually or when significant changes occur to ensure its continued relevance and effectiveness.

Date	Version	Author	Reason for amendment
February 2021 (with annual review thereafter)	5.1	Claire Robinson	Create formalised Data Protection Policy
June 2024	6.0	Claire Robinson	Update Data Protection Policy in alignment with changes to relevant data protection law.
September 2025	6.1	Claire Robinson	Annual Review

1. Introduction

This Data Protection Policy is the overarching policy for data security and protection for Beacon Medical Systems Ltd (hereafter referred to as "us", "we", or "our").

2. Purpose

The purpose of the Data Protection Policy is to support data protection legislation, including the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018) and the changes enacted by the Data (Use and Access) Act 2025.

We recognise and take responsibility for handling personal data. We recognise data protection as a fundamental right and embrace the principles of data protection by design and by default.

3. Scope

This policy applies to Beacon Medical Systems Ltd and all staff, including temporary staff and contractors. All staff, contractors, and temporary workers must complete mandatory data protection training annually and immediately report any suspected data breach or security incident to the DPO.

Included in this policy scope are our data protection principles, commitment to common law and legislative compliance, data protection by design and default procedures and all personal data we process, whether in digital or hard copy format, including special category data.

4. Key Terms

Data Controller
This is the entity that determines the purposes and means of processing personal data. For instance, if you're a business collecting customer data, you are likely the data controller.

Data Processor
A data processor is a person, company, or organisation that processes personal data on behalf of the data controller. They act according to the instructions given by the data controller. This could be a third-party service provider or an internal department within the same organisation as the data controller.

Data Protection Officer
We have appointed a Data Protection Officer to ensure that personal information is kept safe and processed legally. A Data Protection Officer is a designated person or role within an organisation responsible for overseeing data protection strategy and implementation to ensure compliance with data protection laws and regulations.

Data Subject
A data subject is defined as an identifiable individual about whom personal data is processed. This definition is broad and encompasses any living person who can be identified directly or indirectly by reference to an identifier such as a name, an identification number, location data, an online identifier, or factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.

Personal data
Personal data is any information that relates to an identified or identifiable individual. This includes direct identifiers like names and email addresses, as well as indirect identifiers like location data or online usernames. It also encompasses sensitive information such as health data or religious beliefs. Under data protection laws, organisations must handle personal data responsibly, ensuring lawful and fair processing while protecting individuals' rights to privacy and data protection.

Processing
Processing refers to any activity relating to personal data, from beginning to end. It includes the organising, altering, making use of, transferring, combining, holding and destruction of data, either electronically or manually.

Special Category Personal Data
Special category personal data (sometimes referred to as sensitive personal data) is a classification of personal data that is considered particularly sensitive and deserving of extra protection under data protection laws.

5. Data Protection Principles

We will be open and transparent with service users and those who lawfully act on their behalf in relation to their care and treatment. We will adhere to our duty of candour responsibilities as outlined in the Health and Social Care Act 2012.

We will establish and maintain policies to ensure compliance with the Data Protection Act 2018, Human Rights Act 1998, the common law duty of confidentiality, the UK GDPR, and all other relevant legislation.

We will establish and maintain policies for the controlled and appropriate sharing of service user and staff information with other agencies, taking account of all relevant legislation and data subject consent.

Where consent is required for the processing of personal data, we will only rely on consent as a lawful basis where appropriate, ensuring it is informed, explicit, freely given and properly documented. Consent can be withdrawn at any time through clear processes explained to the individual.

We will undertake annual audits of our compliance with legal requirements.

We acknowledge our accountability in ensuring that personal data shall be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation').
- Accurate and kept up to date.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (storage limitation').
- Processed in a manner that ensures appropriate security of the personal data.

We uphold the personal data rights outlined in the Data Protection Act 2018 (UK GDPR):

- The right to be informed.
- The right of access.
- The right to rectification.
- The right to erasure.
- The right to restrict processing.
- The right to data portability.
- The right to object.
- Rights in relation to automated decision making and profiling.

In line with legislation, we employ a Data Protection Officer (DPO) who will report to the highest management level of the organisation. We will support the DPO with the necessary resources to carry out their tasks and ensure that they can maintain expertise. We guarantee that the DPO will not be pressured on how to carry out their tasks, and that they are protected from disciplinary action when carrying out the tasks associated with their role.

6. Underpinning Policies & Procedures

This policy is underpinned by the following:

- Data Quality Policy – outlines procedures to ensure the accuracy of records and the correction of errors.
- Record Keeping Policy – details transparency procedures, the management of records from creation to disposal (inclusive of retention and disposal procedures), information handling procedures, procedures for subject access requests, right to erasure, right to restrict processing, right to object, and withdrawal of consent to share.
- Data Security Policy – outlines procedures for ensuring the security of data including the reporting of any data security breach.
- Business Continuity Plan – outlines the procedures in the event of a security failure or disaster affecting digital systems or mass loss of hardcopy information necessary to the day-to-day running of our organisation.
- Staff Data Security Code of Conduct – contained within our IG Handbook which provides staff with clear guidance on the disclosure of personal information.

7. Data Protection by Design & by Default

We shall implement appropriate organisational and technical measures to uphold the principles outlined above. We will integrate necessary safeguards to any data processing to meet regulatory requirements and to protect individual's data rights. This implementation will consider the nature, scope, purpose and context of any processing and the risks to the rights and freedoms of individuals caused by the processing.

We shall uphold the principles of data protection by design and by default from the beginning of any data processing and during the planning and implementation of any new data process.

Prior to starting any new data processing, we will assess whether we should complete a Data Protection Impact Assessment (DPIA) using the ICO's screening checklist: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/

All new systems used for data processing will have data protection built in from the beginning of the system change.

All existing data processing has been recorded on our Record of Processing Activities. Each process has been risk assessed and is reviewed annually.

We ensure that, by default, personal data is only processed when necessary for specific purposes and that individuals are therefore protected against privacy risks.

In all processing of personal data, we use the least amount of identifiable data necessary to complete the work it is required for, and we only keep the information for as long as it is required for the purposes of processing or any other legal requirement to retain it.

Where possible, we will use pseudonymised data to protect the privacy and confidentiality of our staff and those we support.

8. Responsibilities

Our designated Data Protection Officer is Claire Robinson (Prior Analytics Ltd).

The key responsibilities of the lead are:

- To ensure the rights of individuals in terms of their personal data are upheld in all instances and that data collection, sharing and storage is in line with the Caldicott Principles.

- To define our data protection policy and procedures and all related policies, procedures and processes and to ensure that sufficient resources are provided to support the policy requirements.

- To complete the Data Security & Protection Toolkit (DSPT) annually and to maintain compliance with the DSPT.
- To monitor information handling to ensure compliance with law, guidance and the organisation's procedures and liaising with senior management and DPO to fulfil this work.
- Overseeing changes to systems and processes.
- Monitoring compliance with the GDPR and the Data Protection Act 2018.
- Completing DPIAs.
- Reporting on data protection and compliance with legislation to senior management.
- Liaising, if required, with the Information Commissioner's Office (ICO).
- All data breaches or suspected breaches must be reported immediately following the procedures set out in our Data Security Policy and Incident Management Procedure. The DPO will assess and, where required, report to the ICO within 72 hours."

Our DPO can be contacted by email, phone, or at the following address:
Claire Robinson – dpo@hellopando.com

5 New Street Square, London, United Kingdom, EC4A 3TW

In addition to the Data Protection Officer some key teams and individuals are also responsible for data protection compliance within Beacon Medical Systems Ltd.