Approved by: Board of Trustees
Last updated and approved: February 2025
Date of next review: February 2026

NEOTREE DATA PROTECTION POLICY

1. Interpretation, Purpose and Scope

1.2 Purpose

The purpose of this Data Protection Policy is to outline Neotree's commitment to protecting the privacy and security of Personal Data of (a) our customers and prospective customers, including health-related information collected from newborns and their mothers in low-resource healthcare settings, (b) suppliers and business contacts, (c) employees and workers, including contractors and downstream implementation partners, (d) website users.

Neotree processes Personal Data of our customers and prospective customers to:

- Contribute to research aimed at reducing newborn mortality;
- Empower healthcare professionals and policy makers to deliver high-quality newborn care;
- Support diagnostic decisions and clinical management;
- Provide education and training for healthcare workers; and
- Ensure that every baby is counted and cared for.

Neotree processes Personal Data of suppliers and business contacts to receive their services and to manage its relationship with them.

Neotree processes Personal Data of employees and workers including contractors, upstream partners and downstream implementation partners to:

- Carry out its obligations under the employment or similar agreement with the Data Subjects;
- Comply with its legal obligations as an employer / contracting body;
- Manage its resources in providing its services to customers.

Neotree processes Personal Data of website users to provide its services, to manage requests from users and to communicate with users, and to manage users' accounts.

1.3 Scope

This policy applies to all personal and health-related data collected, processed, and stored by Neotree.

The policy covers data processing activities in all countries where Neotree operates, including Zimbabwe and Malawi. It applies to all Neotree staff, researchers, downstream partners, volunteers, and any third parties who may have access to Neotree data (together referred to as 'personnel').

Neotree staff members must comply with this Data Protection Policy and Related Policies.

2. Legal Basis and Principles

Neotree is committed to complying with all relevant data protection laws and ethical guidelines in the countries where it operates, including but not limited to:

- The UK GDPR
    - Neotree adheres to the principles relating to Processing of Personal Data set out in the UK GDPR which require Personal Data to be:
        (a) Processed lawfully, fairly and in a transparent manner (lawfulness, fairness and transparency). Under UK GDPR, Neotree must Process Personal Data based on the legal bases.
        (b) Collected only for specified, explicit and legitimate purposes (purpose limitation);
        (c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (data minimisation);
        (d) Accurate and where necessary kept up to date (accuracy);
        (e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (storage limitation);
        (f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (security, integrity and confidentiality);
        (g) Not transferred to another country without appropriate safeguards in place (transfer limitation); and
        (h) Made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (Data Subject's rights and requests) where appropriate.

- Ethics Guidelines for Health Research Involving Human Participants in Zimbabwe, published by the Medical Research Council of Zimbabwe (Version 1.4, 30 September 2011)
- Any other applicable national or international data protection regulations.

Neotree reflects how it processes Personal Data of Data Subjects in a privacy notice and reviews its notices regularly (at least yearly) in line with the principles above. Neotree regularly reviews and updates this policy to ensure ongoing compliance with evolving data protection standards and best practices in its healthcare data management.

3. Data Collection and Use

Personal Data of customers and prospective customers

- Data are primarily collected through Neotree's digital platform when healthcare professionals use the Neotree mobile application in neonatal wards to guide the process of caring for the baby and/or mother.
- Data are only collected if they are used to benefit the health and care of the baby and/or mother.
- The data are used directly in the application to support the healthcare professional in the care of the baby, for example by alerting the healthcare professional to a likely condition and cause of treatment. Data are stored in Neotree's databases and visualisation tools. No data should be collected that do not support the care of the baby or mother, or is required for public health benefits in line with the data minimisation principle of UK GDPR.
- A pseudonymised version of the data is aggregated in a database and used by healthcare professionals at a facility level (primary, secondary or tertiary) to help identify issues at e.g. the hospital level and drive improvements of care at that level.
- An anonymised version of the data can be aggregated at a district or country level to support Ministries of Health drive improved healthcare at a district or country level.
- An anonymised version of the data is used to support research into the impact of the Neotree on health outcomes and to train and improve machine learning models to support the caring of the baby and/or mother. This analysis might be performed outside the country where the data was collected. (With the permission of the relevant Ministry of Health who own the data that the anonymised data set was derived from.).

Personal Data of suppliers and business contacts

- Neotree collects Personal data of suppliers and business partners directly from the supplier or business partner organisations, from their websites or other publicly available sources.

Personal Data of employees and workers

- Neotree collects Personal data of employees and workers directly from them, from their former employers, from recruitment agencies and any other third parties that Neotree engages for any necessary background checks.

Personal Data of website users

- Neotree collects Personal data of website users from them directly and via cookies

Personal Data of a Data Subject must be collected only for the specified, explicit and legitimate purposes outlined in this Data Protection Policy and/or relevant privacy notice. It must not be further Processed in any manner incompatible with those purposes.

4. Data Ownership and role of Neotree

- The Neotree software is open source and available under the MIT licence.
- The Neotree software is typically used by Ministries of Health in different countries and specific facilities to support the care of babies and mothers.
- The Ministry of Health of a relevant country that has implemented the technology is typically a Data Controller of Personal Data of customers and prospective customers.
- The Neotree charity often supports as a Data Processor: setting up and running the technology on behalf of the Ministry of Health.
- With the permission of the Ministries, an anonymised version of the data is used by the Neotree team for research purposes: for example to measure the impact that the technology has on health outcomes at a macro level, and to enable the development of machine learning algorithms.
- Neotree is a data controller of employee and worker Personal Data, supplier and business contact data, and of website users.

5. Security Measures

5.1 Commitment to Data Protection

Personal Data of Data Subjects must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

Neotree is committed to implementing and maintaining the highest standards of data protection and security practices, including the sensitive nature of the health data we Process. Our security measures are designed to protect the confidentiality, integrity, and availability of all personal and health-related information collected through our platform, defined as follows:

(a) Confidentiality: only people who have a need to know and are authorised to use the Personal Data can access it;
(b) Integrity: Personal Data is accurate, available, and suitable for the purpose for which it is processed; and
(c) Availability: authorised users are able to access the Personal Data when they need it for authorised purposes.

5.2 Data Access Control

To ensure that Personal Data is accessed only by authorised personnel, Neotree implements strict access control measures:

1. *Strict Access Control (RBAC):* Access rights are assigned based on the principle of least privilege, ensuring that users have access only to the data necessary for their specific roles and responsibilities. Users may only Process Personal Data when performing their roles and responsibilities. Users cannot Process Personal Data for any reason unrelated to their roles and responsibilities.
2. *Regular Access Reviews:* User access rights are periodically reviewed and updated to maintain the principle of least privilege.

5.3 Data Encryption and Storage Limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

To protect health and other sensitive data of customers or prospective customers or employees and workers from unauthorised access during transmission and storage:

1. *Encryption in Transit:* All data transmitted over networks are encrypted using industry-standard protocols (e.g., TLS 1.2 or higher)
2. *Encryption at Rest:* All stored data is encrypted using strong encryption algorithms (e.g., AES-256).

5.4 Data Anonymisation and Pseudonymisation

To minimise the risk of individual identification while maintaining data utility:

1. *Data Minimisation:* Only necessary Personal Data are collected and Processed. Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.
2. *Anonymisation Techniques:* Where possible, data are anonymised by removing all personally identifiable information

3. *Pseudonymisation:* When full anonymisation is not possible, data is pseudonymised by replacing personal identifiers with artificial identifiers.

6. Data Sharing and Third Parties

Generally, Neotree is not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

Neotree may only share the Personal Data it holds with third parties if:

(a) The third party has agreed to comply with the required data security standards, policies and procedures, and put adequate security measures in place; and
(b) a fully executed written data sharing agreement has been obtained in accordance with paragraph 6.3 below.

6.1 Principles of Data Sharing

Neotree recognises the potential benefits of responsible data sharing in advancing newborn healthcare and research. Our approach to data sharing is guided by the following principles:

- *Transparency:* We are open about what data we share, with whom, and for what purposes and inform the Data Subjects of how we handle Personal Data in a form of a privacy notice;
- *Consent:* We only share anonymised data in accordance with the consent provided by the data owner;
- *Necessity:* We share only the minimum amount of data necessary to fulfil the stated purpose;
- *Security:* We ensure that appropriate security measures are in place to protect data during transfer and use by Neotree and by any third parties it engages or shares the Personal Data with; and
- *Accountability:* We maintain oversight of how shared data are used and ensure compliance with our data protection standards.

6.2 Categories of Data Sharing

Neotree may share data under the following circumstances:

- *Research Collaboration:* Sharing de-identified data with academic institutions or research partners to advance neonatal health research;
- *Healthcare Providers:* Sharing patient data with healthcare providers directly involved in the care of newborns and mothers;
- *Public Health Authorities:* Sharing aggregated or de-identified data with public health authorities for disease surveillance and health system planning;

- *Technology Partners:* Sharing data with technology providers who assist in maintaining and improving our digital platform to the extent required for the provision of their services; and
- *Legal Requirements:* Sharing data when required by law, court order, or regulatory authorities.

6.3 Data Sharing Agreements

All data sharing arrangements with third parties are governed by written data sharing agreements that specify:

- The purpose of the data sharing;
- The types of data to be shared;
- The duration of the data sharing arrangement;
- The responsibilities of each party in protecting the data and rights of Data Subjects;
- Restrictions on data use and further sharing; and
- Data destruction requirements upon completion of the stated purpose.

6.4 Vetting of Third Parties

Before sharing Personal Data with any third party, Neotree conducts a thorough vetting process to ensure they meet our data protection standards:

- *Security Assessment:* Evaluation of the third party's data security measures and practices;
- *Compliance Check:* Verification of the third party's compliance with relevant data protection regulations;
- *Contractual Obligations:* Establishment of clear contractual terms regarding data protection responsibilities.

The standards that the third party needs to meet will depend on the nature of the data shared, with a higher standard required where sensitive data is shared (including health data), and a lower (or no standard) where anonymised data is shared.

6.5 Oversight and Auditing

Neotree maintains ongoing oversight of third parties with access to our data where that data is sensitive (i.e. Personal Data):

- *Regular Audits:* Conducting periodic audits of third parties' data protection practices, including their technical security measures;
- *Access Reviews:* Regular reviews of third-party access rights to ensure they remain appropriate; and

- *Incident Reporting:* Requiring third parties to promptly report any data breaches or security incidents.

These measures do not apply in the case of third parties who only have access to anonymised data.

6.6 International Data Transfers

When sharing data internationally, Neotree ensures compliance with relevant data transfer regulations:

- *Adequacy Decisions:* Prioritising data sharing with countries recognised by the UK as providing adequate data protection;
- *Standard Contractual Clauses:* Implementing UK-approved International Data Transfer Agreements where necessary; and
- *Additional Safeguards:* Applying additional technical and organisational measures as required to protect Personal Data during international transfers and when stored in third countries where the results of a transfer impact assessment show such additional safeguards must be taken.

6.7 Data Minimisation and Anonymisation

When sharing Personal Data with third parties, Neotree applies data minimisation and anonymisation techniques:

- *De-identification or anonymisation:* Permanently removing Personal Data before sharing data so that it cannot be re-identified or traced back to the Data Subject;
- *Aggregation:* Sharing Personal Data in aggregate form where individual-level data is not disclosed; and
- *Pseudonymisation:* Using pseudonyms or codes to replace direct identifiers when sharing Personal Data for research purposes.

7. Special Considerations for Health Data

Neotree acknowledges that health data, particularly that of newborns and their mothers, are highly sensitive and is a Special Category of Personal Data and requires exceptional care and protection in their handling. We recognise our ethical and legal obligations to protect these data to the highest standards.

8. Staff Training and Awareness

8.1 Commitment to a Culture of Data Protection

Neotree is committed to fostering a culture of data protection awareness among all staff members. We recognise that effective data protection relies on the knowledge, skills, and vigilance of every individual within our organisation.

Neotree ensures all staff members have undergone adequate training to enable them to comply with data privacy laws, relevant to their roles. We also regularly test our systems and processes to assess compliance.

8.2 Role-Specific Training

In addition to general training, staff members receive specialised training based on their specific roles and responsibilities:

- *Data Handlers:* In-depth training on data minimisation, anonymisation techniques, and secure data processing;
- *IT Staff:* Training on cybersecurity, system maintenance, and security auditing;
- *Research Team:* Specialised training on ethical considerations in health research and data anonymisation techniques; and
- *Management:* Training on oversight responsibilities, risk assessment, and compliance monitoring.

8.3 Feedback and Continuous Improvement

Neotree encourages open communication about data protection practices:

- *Feedback Channels:* Providing easy-to-use channels for staff to submit feedback or raise concerns about data protection practices; and
- *Policy Reviews:* Involving staff in the review and updating of data protection policies and procedures.

Staff members must regularly review all the systems and processes under their control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

9. Compliance and Accountability

9.1 Data Protection Officer (DPO)

Neotree has voluntarily appointed a qualified Data Protection Officer, Yali Sassoon, responsible for:

- Overseeing data protection strategy and implementation, including overseeing this data protection policy and developing related policies and privacy guidelines
- Monitoring compliance with data protection laws and internal policies
- Serving as a point of contact for supervisory authorities.

Please contact the DPO (yali@neotree.org) with any questions about the operation of this Data Protection Policy or the UK GDPR or if you have any concerns that this Data Protection Policy is not being or has not been followed.

9.2 Cooperation with Supervisory Authorities

Neotree is committed to cooperating fully with data protection supervisory authorities by:

- Maintaining open lines of communication with relevant authorities;
- Promptly responding to inquiries or investigations; and
- Implementing recommendations from supervisory authorities.

10. Review and Updates

Neotree is committed to continuously reviewing, monitoring and improving our Data Protection Policy and practices through:

- Regular review and updating of data protection policies and procedures;
- Monitoring of regulatory changes and swift implementation of required updates; and
- Encouraging staff feedback on data protection practices and addressing concerns promptly.

This Data Protection Policy does not override any applicable national data privacy laws and regulations in countries where Neotree operates.

11. Definitions

Data Subject: living, identified or identifiable individual about whom Neotree hold or process Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that Neotree can identify (directly or indirectly) from that data alone or in combination with other identifiers Neotree possesses or can reasonably access. Personal Data includes Special Categories of Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently

removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related Policies: Neotree's policies, operating procedures or processes related to this Data Protection Policy and designed to protect Personal Data.

Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

UK GDPR: the retained EU GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) as defined in the Data Protection Act 2018.