



SHREE VANZA GNATI MANDAL

P. O. BOX 38585, DAR ES SALAAM

Personal Data Privacy Policy for Shree Vanza Gnati Mandal

Preamble

This Personal Data Protection Policy (the "Policy") outlines the commitment of **Shree Vanza Gnati Mandal** (hereinafter referred to as "the Trust," "we," "us," or "our") to protect the privacy and personal data of all individuals with whom we interact, including beneficiaries, settlors, trustees, employees, and third-party service providers.

The Trust recognizes the importance of safeguarding personal data and is dedicated to ensuring compliance with the Personal Data Protection Act of Tanzania (PDPA) and its accompanying regulations, as well as the guidelines issued by the Personal Data Protection Commission (PDPC). This Policy serves as our framework for handling personal data responsibly and transparently.

Overview of the Policy

1.1. Definitions

For clarity, key terms used in this Policy shall have the meanings ascribed to them in the Personal Data Protection Act of Tanzania. Some essential definitions include:

Personal Data: Any information relating to an identified or identifiable natural person (data subject).

Sensitive Personal Data: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

Processing: Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means.

Data Subject: The identified or identifiable natural person to whom the personal data relates.

Data Controller: A person who, either alone or jointly with other persons, determines the purpose and means of processing of personal data.

Data Processor: A person who processes personal data on behalf of the data controller.

PDPC: Personal Data Protection Commission of Tanzania.

1.2. Introduction

The Trust is committed to protecting the privacy and security of personal data entrusted to us. This Policy details our approach to data protection, ensuring that all personal data is collected, processed, stored, and disposed of in accordance with the PDPA and international best practices.

1.3. Purpose

The objectives of this Policy are to:

- a) Establish clear guidelines for the collection, use, storage, and disposal of personal data.
- b) Ensure the Trust's compliance with the Personal Data Protection Act of Tanzania.
- c) Protect the rights and freedoms of data subjects concerning their personal data.
- d) Foster transparency and accountability in the Trust's data processing activities.

1.4. Scope

This Policy applies to all personal data processed by the Trust, whether in electronic or physical form. It covers all trustees, employees, volunteers, contractors, and any third parties acting on behalf of the Trust who may have access to personal data. This Policy applies to all data processing activities undertaken by the Trust within Tanzania and to transborder data flows where applicable.

2. Policy Statements

2.1. Principles of Personal Data Protection

The Trust adheres to the following core principles of personal data protection:

(i) Lawfulness, Fairness, and Transparency:

Personal data is processed lawfully, fairly, and in a transparent manner in relation to the data subject.

(ii) Purpose Limitation:

Personal data is collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

(iii) Data Minimisation:

Personal data collected is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

(iv) Accuracy:

Personal data is accurate and, where necessary, kept up to date. Every reasonable step is taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.

(v) Storage Limitation:

Personal data is 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.

(vi) Integrity and Confidentiality:

Personal data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.

(vii) Accountability:

The Trust, as the Data Controller, is responsible for, and must be able to demonstrate compliance with, the above principles.

2.2. Data Collection and Use

Types of Personal Data Collected:

The Trust may collect various types of personal data, including but not limited to names, contact details, identification documents, financial information, health information (where necessary for beneficiary support), and other relevant data required for the administration of the Trust and its objectives.

Methods of Data Collection:

Data is collected through direct interactions (e.g., application forms, correspondence), from third parties (e.g., legal advisors, financial institutions with consent), and through automated means (e.g., website cookies, if applicable).

Legal Basis for Data Processing:

The Trust processes personal data based on one or more of the following legal grounds:

The explicit consent of the data subject.

- a) Necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

- b) Necessity for compliance with a legal obligation to which the Trust is subject.
- c) Necessity to protect the vital interests of the data subject or another natural person.
- d) Necessity for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Trust.
- e) Necessity for the purposes of the legitimate interests pursued by the Trust or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

2.3. Data Subject Rights

Individuals whose personal data is collected and processed by the Trust have the following rights:

- a) Right to be informed:

The right to be informed about the collection and use of their personal data.

- b) Right of Access:

The right to obtain confirmation as to whether or not personal data concerning them is being processed, and, where that is the case, access to the personal data.

- c) Right to Rectification:

The right to obtain the rectification of inaccurate personal data concerning them.

- d) Right to Erasure (Right to be Forgotten):

The right to obtain the erasure of personal data concerning them under certain conditions.

- e) Right to Restriction of Processing:

The right to obtain restriction of processing under certain conditions.

- f) Right to Data Portability:

The right to receive the personal data concerning them, which they have provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance.

- g) Right to Object:

The right to object, on grounds relating to their particular situation, at any time to processing of personal data concerning them.

h) Rights in relation to automated decision making and profiling:

The right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

2.4. Processing Sensitive Personal Data and/or Genetic or Biometric Data

The Trust will only process sensitive personal data (including genetic or biometric data) when strictly necessary and with explicit consent of the data subject, or where permitted by law (e.g., for substantial public interest, legal claims, medical purposes, or social security). Robust security measures will be implemented to protect such data, ensuring its confidentiality and integrity.

2.5. Consent Management

The Trust outlines procedures for obtaining, managing, and documenting consent within the organization. Where consent is the legal basis for processing, it must be freely given, specific, informed, and unambiguous. Data subjects have the right to withdraw their consent at any time, and the Trust will provide clear mechanisms for doing so.

2.6. Data Security and Storage

The Trust is committed to implementing robust security measures and proper storage practices to ensure the integrity, confidentiality, and availability of personal data. This includes:

- (i) Implementing technical safeguards such as encryption, access controls, and firewalls.
- (ii) Implementing organizational safeguards such as data protection training, clear policies, and regular security audits.
- (iii) Storing personal data in secure environments, whether physical (locked cabinets) or digital (secured servers, cloud services with appropriate data processing agreements).

2.7. Complaints Handling

The Trust has established clear procedures for managing and resolving complaints related to personal data protection. Data subjects can lodge a complaint with the Data Protection Officer (DPO) of the Trust, who will investigate and respond in a timely manner. If the data subject is not satisfied with the resolution, they have the right to lodge a complaint with the Personal Data Protection Commission (PDPC) of Tanzania.

2.8. Roles and Responsibilities of a Data Protection Officer (DPO)

The Trust will appoint a Data Protection Officer (DPO) whose key roles and responsibilities include:

- (i) Informing and advising the Trust and its employees about their obligations under the PDPA and other data protection laws.
- (ii) Monitoring compliance with data protection laws and the Trust's data protection policies.
- (iii) Providing advice regarding Data Protection Impact Assessments (DPIAs) and monitoring their performance.
- (iv) Cooperating with the PDPC and acting as the contact point for the supervisory authority and for data subjects on all issues related to the processing of their personal data.
- (v) The DPO will operate with independence in the performance of their duties.

2.9. Employees Training and Awareness

The Trust is committed to ensuring that all trustees, employees, and relevant personnel understand their responsibilities regarding personal data protection. Regular training and awareness programs will be conducted to equip them with the necessary knowledge and skills to comply with data protection laws and best practices.

2.10. Data Retention and Disposal

The Trust will establish policies and procedures for retaining and disposing of personal data in a manner that ensures compliance with personal data protection laws and minimizes risk. Personal data will not be retained for longer than necessary for the purposes for which it was collected, unless a longer retention period is required or permitted by law. Secure disposal methods will be employed to prevent unauthorized access to disposed data.

2.11. Personal Data Breach Notification

The Trust will outline its approach to identifying, reporting, and addressing personal data breaches in accordance with the Personal Data Protection Act of Tanzania and other relevant regulations. In the event of a personal data breach, the Trust will notify the PDPC without undue delay and, where feasible, not later than seventy-two (72) hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Affected data subjects will also be notified if the breach is likely to result in a high risk to their rights and freedoms.

2.12. Privacy Notes

The Trust will provide clear and concise privacy notices (or privacy statements) to individuals at the point of data collection, informing them about how their personal

data is collected, used, shared, and protected in compliance with the Personal Data Protection Act of Tanzania and other relevant personal data protection regulations.

2.13. Data Protection Impact Assessment (DPIA)

The Trust will outline its approach to conducting Data Protection Impact Assessments (DPIAs) for processing activities that are likely to result in a high risk to the rights and freedoms of natural persons. DPIAs will help ensure that data processing activities comply with data protection laws and mitigate potential risks to individuals' privacy.

2.14. Transborder Flow of Personal Data

The Trust will outline procedures for managing the cross-border transfer of personal data to ensure compliance with the Personal Data Protection Act of Tanzania and other relevant data protection regulations. Personal data will only be transferred outside Tanzania if adequate safeguards are in place, such as standard contractual clauses, binding corporate rules, or if the recipient country ensures an adequate level of protection.

2.15. Automated Processing of Personal Data and Profiling

The Trust will outline its approach to managing automated processing, profiling, and marketing to ensure compliance with the Personal Data Protection Act of Tanzania and to safeguard individuals' rights and freedoms. Data subjects will be informed about any automated decision-making and profiling, and where applicable, have the right to obtain human intervention, express their point of view, and contest the decision.

2.16. Sharing Personal Data

The Trust will outline its policies and procedures for sharing personal data with third parties (e.g., service providers, other trusts, government bodies) to ensure compliance with the Personal Data Protection Act of Tanzania and other relevant data protection regulations. Data sharing agreements will be put in place to ensure that third parties adhere to the same data protection standards.

2.17. Disclosure of Personal Data to Law Enforcement Authorities

The Trust will outline procedures for disclosing personal data to law enforcement authorities to ensure compliance with the Personal Data Protection Act of Tanzania and other relevant legal requirements. Such disclosures will only occur when legally mandated and in a manner that respects the rights of data subjects.

2.18. Use of CCTV cameras and locator technologies

If the Trust utilizes CCTV cameras or locator technologies, it will outline procedures for their use to ensure compliance with the Personal Data Protection Act of Tanzania and other relevant data protection regulations. Clear signage will be displayed, and data collected will be processed for specified, legitimate purposes only (e.g., security).

2.19. Cookies and Online Tracking

If the Trust operates a website or online platforms, it will outline procedures for using cookies and online tracking technologies to ensure compliance with the Personal Data Protection Act of Tanzania and other relevant data protection regulations. Users will be provided with clear information about the use of cookies and given options to manage their preferences.

2.20. Online Privacy Rights for Special Groups

The Trust recognizes that special groups, including children, vulnerable individuals, and individuals with specific needs, require additional protections regarding their online privacy. The Trust will outline procedures to ensure the safeguarding of online privacy rights for these special groups in compliance with the Personal Data Protection Act of Tanzania and other relevant regulations, including obtaining parental/guardian consent where required for children's data.

2.21. Data Protection by Design and by Default

The Trust is committed to integrating data protection measures into the design of systems and processes from the outset and ensuring that privacy considerations are the default setting in data processing activities. This proactive approach aims to minimize data protection risks from the initial stages of any new project or system.

3. Implementation Procedures, Monitoring and Evaluation

The Trust will establish robust measures for the effective implementation, monitoring, and evaluation of this Policy. This will include:

- a) Regular reviews of data processing activities to ensure ongoing compliance.
- b) Internal and external audits of data protection practices.
- c) Maintaining records of processing activities.
- d) Regular updates to this Policy to reflect changes in legislation or best practices.

These measures are crucial for ensuring compliance with the Personal Data Protection Act of Tanzania and maintaining robust data protection practices.

Approval

This policy has been approved by the undersigned and will be reviewed at least annually.

Name: Minesh Nagin Parmar

Title: Chairman of the Trust

Signature: 

Approval Date: 31st March 2026

Review Date: 4th April 2026