

DATA PROTECTION POLICY

1. INTRODUCTION

In light of the magnitude of data being processed in the day to day running of a business it was imperative that a law be enacted to ensure protection of the fundamental right to privacy. In Kenya, the right to privacy is provided under **Article 31 (c) and (d)** of the Constitution of Kenya. From the Constitution of Kenya 2010, The **Data Protection Act of 2019** (the Act) was birthed and thereafter the regulations were formulated to breathe life into the Act.

2. PURPOSE OF THE POLICY

This policy is formulated in accordance to the Data Protection Act 2019 which:

- provides for the right to privacy;
- establishes the Office of the Data Protection Commissioner;
- makes provision for the regulation of the processing of personal data; and
- provides for the rights of data subjects

Therefore, this policy will serve as a guide to the Company to ensure compliance with the Constitution of Kenya, 2010 and the Data Protection Act, 2019, and the Data Protection Regulations in regard to the data it processes. This will in turn ensure that the Company preserves the right to privacy of its clients, employees and stakeholders.

3. DEFINITIONS

Consent - means any manifestation of express, unequivocal, free, specific and informed indication of the data subject's wishes by a statement or by a clear affirmative action, signifying agreement to the processing of personal data relating to the data subject.

Data -means information which—

- (a) is processed by means of equipment operating automatically in response to instructions given for that purpose;
- (b) is recorded with intention that it should be processed by means of such equipment;
- (c) is recorded as part of a relevant filing system;
- (d) where it does not fall under paragraphs (a), (b) or (c), forms part of an accessible record; or
- (e) is recorded information which is held by a public entity and does not fall within any of paragraphs (a) to (d).

Data Protection Impact Assessment - . Means a process of assessing risks in data processing activities. It involves identification of risks, mitigation of risks, management of risks and governance of data protection.

Data Subject - means an identified or identifiable natural person who is the subject of personal data.

Data Commissioner – means a person appointed to oversee the implementation of the Data Protection Act.

Personal Data - means any information relating to an identified or identifiable natural person.

Processing – means any operation or sets of operations which is performed on personal data or on sets of personal data whether or not by automated means, such as

- (a) collection, recording, organisation, structuring;
- (b) storage, adaptation or alteration;
- (c) retrieval, consultation or use;
- (d) disclosure by transmission, dissemination, or otherwise making available; or
- (e) alignment or combination, restriction, erasure or destruction.

Sensitive Personal Data - means data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse or spouses, sex or the sexual orientation of the data subject

4. SCOPE

This policy applies to all personal data collected, processed, stored, and transferred by Mhasibu Housing Company Limited including data handled by third-party service providers. It outlines the organization's commitment to safeguarding the privacy and confidentiality of personal data in compliance with applicable data protection laws and regulations.

5. RIGHTS OF DATA SUBJECT

The Company will inform the data subject of their rights before processing which include the right to:

- (a) be informed of the use to which their personal data is to be put;
- (b) access their personal data in custody of the company
- (c) object or restrict to the processing of all or part of their personal data;
- (d) correction of false or misleading data;
- (e) withdraw consent;
- (f) object to processing of personal data;
- (g) data portability; and
- (h) deletion of false or misleading data about them.
- (i) Object to the processing of their personal data for specific purposes.
- (j) Facilitating data portability by enabling data subjects to receive their personal data in commonly used machine-readable format and allowing data subjects to transmit data.

6. DATA PROTECTION OFFICER

The company may appoint a data protection officer who may be a staff member and who has relevant academic or professional qualifications which may include knowledge and technical skills in matters relating to data protection.

Once appointed, the Company will publish their contact details on the website and communicate them to the Data Commissioner who shall ensure that the same information is available on the official website.

The Company's data protection officer shall—

- (a) advise the Company and the relevant staff on data processing requirements provided under the data protection laws;
- (b) ensure the Company complies with the Data Protection Laws;
- (c) facilitate capacity building of staff involved in data processing operations;
- (d) provide advice on data protection impact assessment;
- (e) co-operate with the Data Commissioner and any other authority on matters relating to data protection; and
- (f) update internal data protection policies, forms and agreements;
- (g) respond to all notices from the Data Commissioner;
- (h) implement mechanisms to handle data subjects' requests and complaints; and
- (i) respond to the various requests and complaints from data subjects in a timely manner.

7. CONSENT

The burden of proof to establish whether consent was obtained lies with the Company. Therefore, the company will provide a detailed consent form (as per annexure 1) which will be signed by the data subjects before processing data and thereafter proper records and register of the consent forms will be maintained.

The Company will also provide a withdrawal of consent form consent form (as per annexure 2) upon request from a data subject.

8. PRINCIPLES OF DATA PROTECTION

While processing data the Company shall Sensitize of the principles of data protection to the Staff by the Data Protection Officer and prepare of a training handbook. The company will be guided by the following principles of data protection which ensure that personal data is:

- (a) processed in a manner that adheres to the right to privacy of the data subject;
- (b) processed in a lawful, fair, and transparent manner;
- (c) collected for explicit, specified, and legitimate purposes and not further processed in a manner incompatible with those purposes;
- (d) adequate, relevant, limited to what is necessary in relation to the purposes for which it is processed;
- (e) collected only where a valid explanation is provided whenever information relating to family or private affairs is required;
- (f) accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay;
- (g) kept in a form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and
- (h) not transferred outside Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject.

9. TRANSFER OF PERSONAL DATA OUTSIDE THE COUNTRY

The Company may only transfer personal data to another country only where there are appropriate safeguards with respect to the security and protection of the personal data including jurisdictions with commensurate data protection laws and where the transfer is necessary —

- (i) for the performance of a contract;
- (ii) for the conclusion or performance of a contract concluded in the interest of the data subject between the and another person;
- (iii) for any matter of public interest;
- (iv) for the establishment, exercise or defence of a legal claim;
- (v) in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or
- (vi) for the purpose of compelling legitimate interests pursued by the company which are not overridden by the interests, rights and freedoms of the data subjects.

10. RETENTION PERIOD AND SCHEDULE

The Company will ensure that it retains the data only as long as may be reasonably necessary to satisfy the purpose for which it is processed. It will also endeavor to conduct regular audits to ensure compliance with the Data Protection Laws.

11. COMMERCIAL USE OF PERSONAL DATA

Processing of personal data for commercial purposes is where personal data of a data subject is used to advance commercial or economic interests, including inducing another person to buy, rent, lease, join, subscribe to, provide or exchange products, property, information or services, or enabling or effecting, directly or indirectly, a commercial transaction. This can be through sending a catalogue through any medium addressed to a data subject;

- (a) displaying an advertisement on an online media site where a data subject is logged on using their personal data; or
- (b) sending an electronic message to a data subject about a sale, or other advertising material relating to a sale, using personal data provided by a data subject.

Personal data, other than sensitive personal data, concerning a data subject will be used for the purpose of direct marketing where—

- (a) the company has collected the personal data from the data subject;
- (b) a data subject is notified that direct marketing is one of the purposes for which personal data is collected;
- (c) the data subject has consented to the use or disclosure of the personal data for the purpose of direct marketing;
- (d) the company provides a simplified opt out mechanism for the data subject to request not to receive direct marketing communications; or
- (e) the data subject has not made an opt out request.

12. DATA PROTECTION IMPACT ASSESSMENT

Where the processing of personal data will highly result in high risk to the rights and freedoms of data subjects, the company will conduct a data protection impact assessment before processing all sensitive personal data. (as per Annexure 5).

13. COLLECTION OF PERSONAL DATA FROM CHILDREN, AND PEOPLE WITH DISABILITY

Data processing based on consent may be exercised as follows:

- (a) **For minors:** Consent must be provided by a person with parental authority or a legal guardian;
- (b) **For individuals with mental or other disabilities:** Consent may be given by a person authorized to act as their guardian or administrator;
- (c) **In all other cases:** Consent may be granted by a person duly authorized by the data subject.

Additionally, when processing data involving a child, it must be done in the best interest of the child and in compliance with the **Children Act of 2022**.

14. MONITORING AND EVALUATING SAFEGUARDS

Appropriate technical and organizational measures will be implemented to ensure the protection of the data subjects rights. The measures include:

- (a) identifying reasonably foreseeable internal and external risks to personal data under the person's possession or control;
- (b) establishing and maintaining appropriate safeguards against the identified risks;
- (c) pseudonymisation and encryption of personal data;
- (d) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- (e) verifying that the safeguards are effectively implemented; and
- (f) ensuring that the safeguards are continually updated in response to new risks or deficiencies.

While considering the appropriate technical and organizational measures, the Company will consider the following:

- (a) the state of technological development available;
- (b) the cost of implementing any of the security measures;
- (c) the special risks that exist in the processing of the data; and
- (d) the nature of the data being processed.

15. NOTIFICATION AND COMMUNICATION OF BREACH

In the event of a data breach, the company will follow a structured response process to address the breach promptly, assess its impact, and notify the relevant parties. The procedures are as follows:

1. Identifying and Containing the Breach

As soon as a potential breach is detected, immediate action will be taken to identify the source and scope of the breach. Steps will be taken to contain the breach to prevent further data loss or unauthorized access. This may involve isolating affected systems, suspending compromised accounts, or disabling access to compromised data.

2. Assessing Risks and Consequences

A thorough assessment will be conducted to evaluate the potential risks and impact of the breach on data subjects. This includes determining the type and sensitivity of the data affected, the potential for identity theft or fraud, and any other possible harm to individuals or the organization.

3. Notification of the Supervisory Authority and Affected Data Subjects

The company will notify the appropriate supervisory authority within **72 hours** of becoming aware of the breach, in accordance with legal obligations. If the breach is likely to result in a high risk to the rights and freedoms of data subjects, they will also be informed within the same time frame.

The notification to the supervisory authority will include:

- A description of the nature of the breach, including the categories and approximate number of data subjects and records affected.
- Contact information for the Data Protection Officer or other point of contact.
- The likely consequences of the breach.
- Measures taken or proposed to address the breach and mitigate its effects.

For affected data subjects, the communication will:

- Explain the nature of the breach and its likely consequences.
- Provide clear steps individuals can take to protect themselves, such as changing passwords or monitoring for suspicious activity.
- Offer guidance on how they can obtain further information or assistance.
- Provide contact details for the Data Protection Officer or a designated point of contact.

4. Mitigating the Risks

In parallel with the notification process, [Company Name] will take immediate actions to mitigate the risks associated with the breach. This could involve restoring data from backups, strengthening access controls, or enhancing system security to prevent further exposure.

5. Preventing Future Breaches

Following the resolution of the breach, [Company Name] will review the incident to determine the root cause and take corrective actions to prevent similar breaches in the future. This may include updating security protocols, conducting staff training, or implementing additional monitoring measures.

6. Documenting the Incident and Response

All breaches will be thoroughly documented, including details of the breach, actions taken to address it, and measures implemented to prevent recurrence. This documentation will be maintained as part of [Company Name]'s compliance records and made available to regulatory authorities if required.

The employees should also report to the company within **forty-eight hours** incase of breach and also ensure that they comply with this policy.

16. SECURITY AND RECORD KEEPING

1. This is to protect unauthorized access by having access control and authentication mechanisms.
2. Encryption of personal data to protect against unauthorized disclosure.
3. Regular backups and disaster recovery procedures to ensure the availability of personal data.
4. Monitoring and logging of access to personal data to detect and respond to security incidents.

17. COMPLAINTS HANDLING MECHANISMS

The Company will put in place mechanisms to receive and resolve complaints and requests from data subjects (as per annexure 6).

18. ROLES AND RESPONSIBILITIES

18.1 BOARD OF DIRECTORS

The Board of Directors will ensure that the Company:

- is registered as Data Handlers;
- appoints a data protection officer;
- is regularly trained to ensure continued compliance;
- reports any incident of breach to the Data Commissioner;
- incorporates a data protection clause in employment contracts;
- engage with third parties who have complied with the Data Protection Laws;
- enter into data protection agreements with clients; and
- has appropriate technical and organizational safeguards to preserve the integrity of the rights of data subjects.

18.2 DATA PROTECTION OFFICER

Once appointed, the Data Protection Officer shall undertake the roles and responsibilities outlined in Clause 6.

18.3 ALL STAFF

All staff must:

- abide by this data protection policy;
- inform the company in case of any breach;
- attend all training opportunities on Data Protection as availed by the company.


19. REVIEW

This policy shall be reviewed after every **three (3)** years or as may be necessary in order to be consistent with any amendments to the legal and regulatory framework.

APPROVED BY

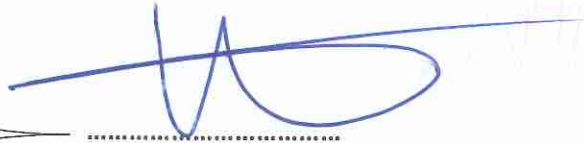
For and On Behalf of **MHASIBU HOUSING COMPANY LIMITED**

Director



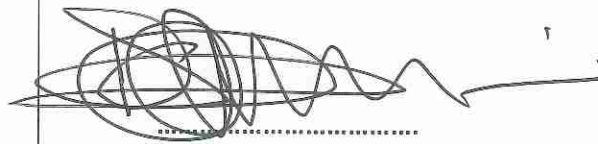
A handwritten signature in black ink, consisting of a large, stylized initial 'M' followed by several loops and a horizontal stroke.

Director



A handwritten signature in blue ink, featuring a large, stylized initial 'M' followed by several loops and a horizontal stroke.

Director /CEO/ Secretary



A handwritten signature in black ink, consisting of a large, stylized initial 'M' followed by several loops and a horizontal stroke.