
DATA PROTECTION POLICY

INTRODUCTION

Data Protection Policy contains 4 policies namely:

- Employee Data Handling Policy
 - Data Retention & Disposal Policy
 - Data Subject Handling Right Policy
 - Data Breach Response Policy
- Employee Data Handling Policy for Home Afrika Limited outlines the company's commitment to responsibly collecting, processing, storing, and protecting employee personal data in compliance with the Data Protection Act, 2019 of Kenya. The policy ensures that employee data is only accessed by authorized personnel for legitimate business purposes, maintained with accuracy, and safeguarded against unauthorized access, disclosure, or loss. Employees are informed of their data rights, including access, objection, correction, and deletion, and the company upholds transparency and accountability in all data handling practices to foster trust and legal compliance.
- Data Retention & Disposal Policy for *Home Afrika Limited* outlines the company's commitment to managing personal and company data responsibly by retaining information only for as long as it is legally or operationally necessary. The policy ensures that data is categorized, stored securely, and retained in accordance with applicable laws, such as tax, employment, and real estate regulations. Once data is no longer required, it is securely disposed of through methods such as permanent deletion of digital files and shredding of physical documents, ensuring the protection of sensitive information and compliance with data privacy obligations.
- Data Subject Handling Rights Policy for *Home Afrika Limited* ensures that all individuals whose personal data is collected, stored, or processed by the company are able to exercise their rights under applicable data protection laws, such as the right to access, object, correct, delete, or restrict the use of their data. Home Afrika is committed to processing personal data lawfully, transparently, and for legitimate purposes only. The company provides clear procedures for submitting data access requests and responds promptly within the stipulated timeframe. Additionally, Home Afrika ensures that personal data is kept secure and that individuals are informed of their rights and how to exercise them, promoting trust and accountability in all data handling practices.
- Data Breach Response Policy outlines how an organization identifies, manages, contains, investigates, and communicates any incident where personal or sensitive data is accessed, disclosed, or lost without authorization. This policy helps ensure timely action to reduce harm to affected individuals and to comply with data protection laws and regulations such as the Data Protection Act (Kenya, 2019).

1. Introduction

Home Afrika Limited (HAL) recognizes that handling personal data appropriately is critical and has adopted appropriate data systems, privacy, and security measures to ensure that it shall not knowingly violate the rights of data subjects through its processing and handling of data.

This Data Protection Policy is based on globally accepted, basic principles on data protection. HAL recognizes data protection as a foundation of trustworthy relationships necessary to build reputation as a credible organization. This policy is designed to be consistent with Kenyan and other international laws and regulations including:

- ☐ The Data Protection (General) Regulations, 2021
- ☐ The Kenya Data Protection Act, No. 24 of 2019 and Regulations
- ☐ Kenya Access to Information Act No. 31

This policy provides guidance on procedures to secure individuals' personal data, regulate the collection, usage, transfer, and disclosure of the said data. The definition of terms used in this policy have been listed in appendix A.

2. Policy Statement

Home Afrika Limited has a responsibility to protect confidential, restricted, and/or sensitive data from unwarranted disclosure, loss, or damage to avoid adversely affecting our staff, shareholders and clients from whom we collect data. Handling personal data in an ethical manner is in line with HAL's values and we will apply all necessary to ensure that the rights of individuals are protected.

3. Purpose of the Policy

3.1. The purpose of this policy is to lay foundation to enforce **Article 31** of the Constitution of Kenya, by developing privacy and data protection measures for Home Afrika staff, shareholders, clients and third parties from whom we collect data from.

3.2. This Policy informs on the management of Personal Data in the information life cycle and the commitment of Home Afrika to protect the Personal Data including the Personal Sensitive Data.

3.3. The objectives of this policy are:

3.3.1. To inform the development of Data Protection laws and facilitate statutory and regulatory compliance and enhance effective application of the proposed laws in Kenya.

3.3.2. To comply with the international good practice and ensure consistency in practices

and procedures in developing and administering the Data Protection laws.

3.3.3. To ensure effective protection and management of Personal Data by identifying, assessing, monitoring and mitigating privacy risks in activities involving the collection, retention, use, disclosure and disposal of Personal Data.

3.4. This policy will establish an independent oversight authority that will ensure compliance of the policy and sound management practices to safeguard the rights of the data subjects.

4. Scope

The policy applies to:

- a) To all Home Afrika representatives i.e. current/ prospective staff members, shareholders, clients, contractors, board members and third parties;
- b) All personal data processing Home Afrika Limited carries out for others (where Home Afrika Limited is the ‘Processor’ for the personal data being processed); and
- c) All formats, e.g. printed and digital information, text and images, documents and records, data and audio recordings.

5. Data Minimization

5.1. HAL shall not process any personal data for a purpose for which it did not obtain consent. Should such a need arise, then consent must be obtained from the data subject.

5.2. HAL will collect and process data that is adequate and relevant in the implementation and management of its services. This data includes:

- 5.2.1. Personal information including, but not limited to, name, gender, race, family and social background, signatures, contact details, photographs and/or video recordings, passport and other travel-related information, education and training records, employment and financial records;
- 5.2.2. Any other personal data routinely collected by HAL in the course of its operations, including but not limited to recruitment and other HR processes, provision of ICT support, finance functions and any other activities involving the collection of personal data. This Policy applies to personal data in HAL’s possession, whether collected from individuals internally or externally across the relevant functional categories;
- 5.2.3. Personal data of employees/applicants: The Company collects and processes personal and Special Category data of job applicants and employees as prescribed in the Data Protection Act 2019. The information is transmitted between and among internal units and divisions for necessary operational purposes.

5.2.4. Personal data of current/prospective fellows: The Company will collect personal and Special Category of Data for prospective or enrolled in order to implement and manage all services and processes relating to its fellows, without which, the Company may be unable to provide its services to these individuals or others.

5.3.Data must only be collected for the performance of duties and tasks; staff must not request data subjects to provide personal data unless that is strictly necessary for the intended purposes;

5.4.The Data Protection Officer must ensure that they delete, destroy, or anonymize any personal data that is no longer needed for the specific purpose for which they were collected.

6. Principles for Data Protection

To comply with the policy, information must be collected and used fairly, stored securely and not disclosed to any other person unlawfully. HAL shall adhere to the global best practices in data protection as set out in statutory provisions and international laws and regulations. These principles include:

6.1.*Privacy*: HAL recognizes the right of a data subject to have control over how his or her personal data is collected, used, and/or disclosed. The company will only process data provided by a data subject willingly and, or with a legal basis as required by the law.

6.2.*Confidentiality*: The Company will take reasonable measures to ensure that data in its possession is kept safe and only accessed by authorized individuals.

6.3. *Integrity*: The Company will maintain accurate records and where required, take necessary steps in providing the assurance of data accuracy and consistency of data in its possession.

6.4. *Autonomy*: The Company recognizes and protects the rights of data subjects to make informed decisions about when to have their data collected and for what it may be used for. The company will put in place measures that enable data subjects to exercise these rights.

6.5. *Justice*: HAL will process all data that is in its possession lawfully, fairly, and in a transparent manner. In this regard, the Company will collect personal data for specified, explicit, and legitimate purposes.

Related policies;

- ☐ HAL ICT Policy
- ☐ HAL Privacy Policy
- ☐ HAL Legal Compliance & Ethics Policy

Employee Data Handling Policy

At Home Afrika Ltd, we are committed to protecting the privacy, confidentiality, and integrity of employee personal data. As a real estate company handling sensitive information, we recognize the importance of complying with data protection laws and maintaining high standards in managing employee data.

This **Employee Data Handling Policy** outlines how we collect, use, store, and protect personal data of our employees throughout their employment lifecycle.

1. Data Collection

We collect personal data strictly for legitimate business, legal, and human resource purposes. This includes but is not limited to:

- Full name, contact information, and identification details
- Employment history, education background, and references
- Bank details for payroll purposes
- Medical and emergency contact information
- Performance records and disciplinary actions

2. Use of Data

Employee data is used for:

- Recruitment and onboarding
- Payroll processing and statutory compliance
- Performance evaluation and career development
- Internal communication and company benefit administration
- Legal obligations and organizational planning

3. Data Storage and Security

All employee data is securely stored in digital and/or physical formats, with access restricted to authorized personnel only. We employ appropriate security measures including:

- Password-protected systems and encrypted databases
- Secure document storage and disposal procedures
- Access control protocols for HR and administrative teams

4. Data Sharing

Employee data will only be shared with:

- Authorized internal departments
- Statutory bodies (e.g., KRA, NSSF, NHIF) as required by law
- Third-party service providers (e.g., payroll processors, medical insurers) under strict confidentiality agreements

5. Employee Rights

Employees have the right to:

- Access their personal data held by the company
- Request correction or deletion of inaccurate or outdated information
- Withdraw consent where applicable
- Report concerns regarding misuse of data

6. Retention and Disposal

Employee data is retained only as long as necessary for legal and operational needs. Once no longer required, data is securely disposed of to prevent unauthorized access.

Data Subject Handling Rights Policy

1. Purpose

The purpose of this policy is to ensure that Home Afrika Ltd respects and facilitates the rights of data subjects in accordance with Kenya's Data Protection Act, 2019 and any other relevant data privacy laws.

2. Scope

This policy applies to all personal data collected, processed, and stored by Home Afrika Ltd in the course of its real estate operations. It covers clients, employees, suppliers, and any other data subjects whose data is handled.

3. Data Subject Rights Covered

Home Afrika Ltd recognizes the following rights of data subjects:

- **Right to be Informed:** Individuals have the right to know how their data is being collected, used, and stored.
- **Right of Access:** Individuals can request access to their personal data held by the company.
- **Right to Rectification:** Individuals can request correction of inaccurate or incomplete data.
- **Right to Erasure:** Also known as the 'right to be forgotten'; individuals can request deletion of their personal data in certain cases.
- **Right to Restrict Processing:** Individuals can request to limit how their data is used.
- **Right to Data Portability:** Individuals can request to receive their data in a structured, commonly used format.
- **Right to Object:** Individuals can object to their data being used for certain purposes (e.g. marketing).
- **Rights in relation to automated decision-making and profiling:** Individuals can ask for human intervention or express concerns about automated decisions that affect them.

4. Request Handling Procedure

- All data subject requests must be submitted via the official **Data Request Form** available on the Home Afrika Ltd website or at our offices.
- Requests will be acknowledged within **7 working days**.
- The company will respond to the request within **30 calendar days**, unless an extension is required.
- Identity verification will be conducted to ensure the request is made by or on behalf of the rightful data subject.

5. Roles and Responsibilities

- The **Data Protection Officer (DPO)** is responsible for overseeing compliance with this policy and responding to data subject requests.
- All employees must cooperate with the DPO in ensuring data rights are upheld.

6. Data Security

Appropriate technical and organizational measures are in place to secure personal data against unauthorized access, loss, or destruction, especially during rights execution.

7. Complaints and Appeals

If a data subject is dissatisfied with how their request was handled, they may:

- Submit a written complaint to the Data Protection Officer.
- File a complaint with the **Office of the Data Protection Commissioner (ODPC)** in Kenya.

Data Retention & Disposal Policy

1. Purpose

This policy provides guidelines for retaining and securely disposing of data collected, processed, and stored by Home Afrika Ltd in the course of its real estate operations. It ensures compliance with relevant data protection laws and supports operational efficiency.

2. Scope

This policy applies to:

- All employees, contractors, and third parties handling data on behalf of Home Afrika Ltd
- All forms of data including physical documents, digital records, emails, customer data, property information, contracts, and financial records

3. Data Retention Principles

- **Lawful Retention:** Data will be retained for the minimum period required by law, contract, or business need.
- **Purpose Limitation:** Data will only be kept as long as necessary to fulfill the purpose for which it was collected.
- **Data Minimization:** Only essential information will be stored.
- **Storage Security:** Data will be stored securely to prevent unauthorized access, alteration, or loss.

4. Retention Periods

Data Type	Retention Period	Reason
Customer records (buyers, sellers, tenants)	7 years	Legal, contractual obligations
Property transaction documents	7 years	Legal/tax compliance
Employee records	5 years after departure	HR, legal references
Financial records (invoices, receipts)	5 years	Audit and tax regulations
Marketing data (e.g. email lists)	2 years	Consent-based marketing
Email correspondence	3 years	Business continuity

Note: Some records may be retained longer if subject to legal disputes or investigations.

5. Data Disposal Procedures

- **Digital Records:** Secure deletion using data wiping or shredding software
- **Physical Documents:** Shredded or incinerated under supervision
- **Devices/Storage Media:** Wiped and physically destroyed before disposal
- **Third Parties:** Disposal must follow the same standards and be contractually enforced

6. Roles & Responsibilities

- **Data Protection Officer (DPO):** Oversees policy implementation and compliance
- **Department Heads:** Ensure departmental data retention practices align with policy
- **Employees:** Follow procedures for data storage and secure disposal

Data Breach Response Policy

Data Breach Response Policy outlines how an organization identifies, manages, contains, investigates, and communicates any incident where personal or sensitive data is accessed, disclosed, or lost without authorization. This policy helps ensure timely action to reduce harm to affected individuals and to comply with data protection laws and regulations such as the Data Protection Act (Kenya, 2019).

1. Purpose

This policy establishes procedures for detecting, reporting, managing, and recovering from data breaches affecting Home Afrika Ltd. It aims to:

- Minimize damage and protect data subjects' rights.
- Ensure legal and regulatory compliance.
- Maintain stakeholder trust.

2. Scope

This policy applies to all employees, contractors, consultants, vendors, and third parties who process, handle, or have access to personal data or confidential information of Home Afrika Ltd.

3. Definition of a Data Breach

A **data breach** is any incident that results in unauthorized access, disclosure, alteration, or destruction of personal or sensitive data. Examples include:

- Loss or theft of a device containing customer data.
- Hacking or ransomware attack.
- Accidental emailing of personal information to the wrong recipient.

4. Roles and Responsibilities

- **Data Protection Officer (DPO):** Coordinates breach response and reports to the Office of the Data Protection Commissioner (ODPC).
- **IT Department:** Investigates and mitigates technical aspects of breaches.
- **All Staff:** Must report any suspected or known data breach immediately.

5. Reporting a Breach

All suspected or confirmed data breaches must be reported **within 24 hours** to the DPO or IT Department using the internal breach reporting form or designated communication channel.

6. Breach Assessment & Containment

Upon notification, the DPO and IT team will:

- Assess the nature and scope of the breach.
- Contain the breach to prevent further loss.
- Secure affected systems and data.

7. Notification Obligations

If a breach is likely to result in harm or risk to individuals:

- A report will be made to the **ODPC** within **72 hours** of detection.
- Affected individuals will be notified with details of the breach and guidance on protecting themselves.

8. Investigation and Documentation

The incident will be documented, including:

- Timeline of events.
- Data affected.
- Actions taken.
- Recommendations for prevention.

A final report will be kept securely by the DPO.

9. Post-Breach Review

After resolving the breach:

- Conduct a review of the response.
- Update security measures and staff training.
- Adjust policies and procedures as necessary.

10. Disciplinary Action

Failure to report or comply with this policy may lead to disciplinary action, up to and including termination of employment or contract.

Roles and Responsibilities

All HAL representatives have a role to play in ensuring compliance with this Policy. Effective Data protection requires the participation and support of every HAL employee and affiliate who deals with data and data systems. It is the responsibility of every user to familiarize themselves with this policy and adhere to it.

The following individuals have specific roles in relation to the Company's Data Protection Policy as below:

The board of directors

- ☐ Ensure the Company keeps pace with evolving data protection trends and practices.

- ☐ Ensure that potential risks are monitored and appropriate mitigation efforts are put in place.
- ☐ Bolster management's ability to apply appropriate safeguards to help minimize data breaches and other privacy mishaps, third party lawsuits, and potential negative reputational risk.

Management team

- ☐ Oversee the implementation of the Policy by developing appropriate programs and guidelines, establishing systems and processes to protect personal data in the Company's possession.
- ☐ Ensure that HAL representatives are sensitized on the Policy and compliance procedures.
- ☐ Exercise appropriate oversight to ensure that the Company adequately assesses data protection risks and implements risk mitigation procedures and processes.
- ☐ Monitor trends in data protection and institute appropriate measures.

Data measurement and evaluation team

- ☐ Ensure compliance with the Company ICT policy in the development of data management, processing, and storage tools and platforms
- ☐ Liaise with the DPO to ensure the safety of personal research data
- ☐ Oversee the Company's data-sharing systems and processes, ensuring compliance with laws and regulations governing ethical use of human subjects' data.

Data Protection Officer

- ☐ Advise the organization and HAL representatives on data processing requirements provided under the DPA 2019 or any other written law.
- ☐ Ensure on behalf of the organization that the DPA is complied with.
- ☐ Facilitate capacity building of staff involved in data processing operations.
- ☐ Record all data breaches and notify the Office of the DPC within 72 hours, where it is established that the breach may result in real harm to affected data subject(s).
- ☐ Conduct a data protection impact assessment as required by the DPA 2019 and related regulations.
- ☐ Develop databases/software used to safely capture, manage, store data collected within the organization.

Legal Officers

- ☐ Review and advise on any changes in the law relating to data protection
- ☐ Draft and review contracts with partners and third parties to ensure compliance with the data protection policy.
- ☐ Ensure contracts with partners embody Data Protection principles.

ICT Officers

- ☐ Notify relevant staff in case of a data breach
- ☐ Secure data from loss, unauthorized access, and inconsistencies.
- ☐ Ensure data availability and accessibility.

All HAL Staffs

- ☐ Handle data related to the organization as required by the applicable laws and align with the

principles outlined in this policy.

☐ Report data incidences, breaches, and malpractice to the DPO within 24 hours of being aware.

Non-Compliance

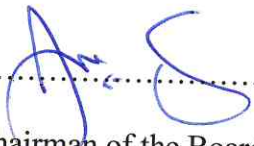
Disciplinary measures will be taken against HAL staff and partners who knowingly attempt to circumvent the administrative, physical, and technical safeguards that have been put in place to protect personal data of any type. Disciplinary measures will be as outlined in the HR Policy.

NB: Disciplinary action does not preclude formal legal action by the affected or referral by the Center to government authorities in accordance with the law.

Policy Revision

This policy is subject to revision whenever legal, pragmatic, or technological developments make revision necessary. In any case, the Policy will be reviewed at least every three years.

Approved by the Board of Directors on the14th..... Day of July.....2026


.....
Chairman of the Board

.....14/07/2026.....
Date

Seconded by:


.....
Director

.....14/07/2026.....
Date