

KENBRIGHT ACTUARIAL AND FINANCIAL SERVICES LIMITED

DATA PROTECTION POLICY

INTERNAL DOCUMENT

VERSION 1.0

JANUARY 2025

KAFS POLICY

kenbright

Kenbright Actuarial & Financial Services Limited
26th Floor- Prism Towers – 3rd Ngong Avenue
P. O. Box 28281 – 00200
Nairobi, Kenya
kafs@kenbright.co.ke

DOCUMENT TRACKING

Revision History			
Version	Author	Date	Revision
1.0	Kenbright Actuarial and Financial Services Limited	January 2025	Creation

Prepared for:

Kenbright Actuarial & Financial Services Limited
26th Floor, Prism Towers
3rd Ngong Avenue, Upperhill
P.O Box 28281 - 00200
Nairobi, Kenya

OUR REF

\\Kenbright\\Policy Documents\\Data Protection Policy

DOCUMENT PURPOSE

The document has been produced to serve as the Data Protection Policy for staff working under Kenbright Actuarial and Financial Services Limited

DOCUMENT OWNERSHIP

The owner of this document is Kenbright Actuarial and Financial Services Limited

TABLE OF CONTENTS

1	INTRODUCTION.....	5
	Purpose	5
	Scope.....	5
	Policy Statement	5
	Principles of Data Protection	5
	Appointment of a Data Protection Officer.....	6
	Data Protection Officer Roles	6
2	PRINCIPLES OF DATA PROTECTION	7
	Principle 1: Lawfulness, Fairness and Transparency.....	7
	Principle 2: Purpose Limitation.....	7
	Principle 3: Data Minimization	7
	Principle 4: Accuracy.....	7
	Principle 5: Storage Limitation	8
	Principle 6: Integrity and Confidentiality.....	8
	Principle 7: Accountability	8
3	COLLECTION AND PROCESSING OF DATA	9
	Data Collection	9
	Rights of a Data Subject	9
	Lawful Processing of Data.....	10
	Safeguards and Security of Data.....	10
	Personal Data Relating to Health	10
	Rectification or Erasure	10
	Notification & Communication of Breach.....	10
	Training and Awareness.....	11
	General Penalty.....	11
	Enforcement.....	11
4	ROLES AND RESPONSIBILITY LEVELS.....	Error! Bookmark not defined.
	Responsibility for the Success of the Policy	12
	Board of Directors.....	12
	Management.....	12
	Employees	12
5	APPROVAL	14

ABBREVIATIONS

NAME	DEFINITION
Agency	A person who collects or processes personal data
Data	Any information which is; Processed by means of equipment operating automatically in response to instructions given for that purpose. Recorded with the intention that it should be processed by means of such equipment. Recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system. Recorded information which is held by a public entity
Data Controller	Any staff, consultant or director who raises a Concern
Data Processor	A person, public authority, agency or other body which processes personal data on behalf of the data controller.
Data Subject	A person from whom personal data is obtained
Identifiable Natural Person	A 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 to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or social identity
KAFS	Kenbright Actuarial & Financial Services Limited
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

1 INTRODUCTION

Purpose

- 1.1. The objective and purpose of this document is to give a detailed outline of how KAFS works towards managing and protecting personal data of our clients, employees, and any other relevant third parties in line with:
- a) The Data Protection Act, 2019;
 - b) the Actuaries Code; and
 - c) Technical Actuarial Standards.

Scope

- 1.2. This policy applies to all employees of KAFS, either permanent, temporary, consultants as well as the Board and other stakeholders of the company regardless of their location.

Policy Statement

- 1.3. Kenbright Actuarial and Financial Services Limited is committed to providing innovative risk and financial advisory solutions in a manner that adheres to the laws and regulations governing the sector. Protecting and properly managing data plays a central part in fulfilling this mandate.
- 1.4. KAFS recognizes the constitutional right of every individual to have their data, both personal and sensitive remain confidential and undisclosed as we work to nurture a culture where trust, accountability and transparency when handling data are upheld.
- 1.5. KAFS will ensure that all data collected, received and processed by the company is done in line with all the relevant legislation governing data and its use in all jurisdictions where KAFS operates in. Any breach of this data protection policy may lead to disciplinary action including and up to termination of employment or contractual terms.

Principles of Data Protection

- 1.6. There have been established globally principles that govern how data is protected and managed which are as highlighted below:
- a) Lawfulness, fairness and transparency
 - b) Purpose limitation
 - c) Data minimization
 - d) Accuracy
 - e) Storage limitation
 - f) Accountability
 - g) Integrity and confidentiality

Appointment of a Data Protection Officer

- 1.7. There will be in KAFS a natural person appointed to be the data protection officer who shall be in charge of protecting and managing all data related to and handled by/in KAFS.
- 1.8. The person should have the required academic or professional qualifications which may include knowledge and technical skills in matters relating to data protection.
- 1.9. The data protection officer shall also be in charge of protecting and managing all data for KAFS subsidiaries in both Uganda and Tanzania.
- 1.10. A Data Protection Officer may be a staff member of the Data Controller or Data Processor and may fulfil other tasks and duties provided that any such tasks and duties do not result in a conflict of interest.
- 1.11. A Data Controller or Data Processor shall publish the contact details of the Data Protection Officer and communicate them to the Data Commissioner.

Data Protection Officer Roles

- 1.12. The responsibility of the data protection officer include but not limited to:
 - a) Advise KAFS on data processing requirements provided under the Data Protection Act or any other written law;
 - b) Serve as the point of contact between the regulatory authority, KAFS, the data controllers and the data subjects;
 - c) Facilitate capacity building of staff involved in data processing operations;
 - d) Provide advice on Data Protection Impact Assessment;
 - e) Cooperate with the Data Commissioner and any other authority on matters relating to data protection; and
 - f) Ensure timely registration with the Office of the Data Protection Commissioner.

2 PRINCIPLES OF DATA PROTECTION

- 2.1. The principles of data protection govern how data should be used and processed. KAFS is committed to maintain them when handling data.
- 2.2. Below is a detailed description of how each will be implemented in KAFS:

Principle 1: Lawfulness, Fairness and Transparency

- 2.3. All data handled in KAFS will be done so in adherence to all the laws and regulations governing data with regards to the jurisdiction under which the data is applicable to.
- 2.4. Adherence to this policy is mandatory for all people working under KAFS as specified under the Scope of this policy.
- 2.5. Any breach of this policy will be treated with urgency and the seriousness it deserves with penalties being given as specified in the Acts governing data protection.
- 2.6. The data protection officer will have the responsibility of ensuring maximum possible compliance of KAFS and its employees to the data protection Acts and regulations.

Principle 2: Purpose Limitation

- 2.7. KAFS will disclose all reasons for request and use of data and should use the data only for specified purposes.
- 2.8. The data compliance officer should review all data request files required to be sent out to clients and any other requests for data made by the data processors at KAFS.
- 2.9. The officer should also ensure that data is not used for any purpose that is not consented to when acquiring the data.

Principle 3: Data Minimization

- 2.10. Any data collected and received is limited to what is necessary for the specified and legitimate purposes for which it is processed.
- 2.11. The data processors at KAFS should not request/collect any unnecessary data or store any of it beyond what is required to carry out their work.

Principle 4: Accuracy

- 2.12. All data processed at KAFS should be accurate and up to date in order to make the most current and meaningful analysis out of it.
- 2.13. Where there are any inaccuracies or queries on the data, the data processors should seek clarity from the client as soon as reasonably practicable.
- 2.14. The data protection officer should oversee the erasure of any inaccuracy, inconsistent or out of date data in accordance with this policy.

Principle 5: Storage Limitation

- 2.15. All data at KAFS should not be stored for a period longer than is required and/or consented to during request and acquisition of the data.
- 2.16. This should be done in accordance with the company's data retention procedures under the Data Management Policy.
- 2.17. The data protection officer should regularly assess the data and give a report on the storage and retention of data which has already been used.

Principle 6: Integrity and Confidentiality

- 2.18. KAFS should implement industry best practices that ensure the security and protection of data against unauthorized access and/or use and any unlawful processing.
- 2.19. There should also be established and implemented mechanisms that guard against accidental loss, damage or destruction of data which should include strong data systems, routine data backups and recovery plans aimed at reducing downtime to ensure that data subjects have access to data uninterrupted.

Principle 7: Accountability

- 2.20. KAFS will take responsibility for all personal data it handles.

3 COLLECTION AND PROCESSING OF DATA

Data Collection

3.1. KAFS will collect its data from the following sources:

- a) Clients/customers including insurance companies; and
- b) Publicly available data.

3.2. KAFS collects data for specified reasons such as:

- a) Carrying out actuarial work, as defined under the Actuarial Work Review policy for KAFS, for clients who majorly are the insurance companies;
- b) Carrying out research; and
- c) Ensuring compliance with legal obligations.

3.3. Collection of data from another source is necessary:

- a) For the prevention, detection, investigation, prosecution and punishment of crime;
- b) For the enforcement of a law which imposes a pecuniary penalty; and
- c) For the protection of the interests of the data subject or another person.

Rights of a Data Subject

3.4. A data subject has a 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 data controller or data processor;
- c) Object to the processing of all or part of their personal data;
- d) Correction of false or misleading data; and
- e) Deletion of false or misleading data about them.

Lawful Processing of Data

3.5. KAFS processes data based on the following lawful basis:

- a) Contractual Obligation – KAFS will process personal data with the aim of fulfilling contractual obligations with insurance companies;
- b) Legal Obligation – data processing is done to fulfill legal obligation by insurance companies as required by the Insurance Regulatory Authority ('IRA') Kenya;
- c) Public interest – the processing is necessary for insurance companies to give a report to their stakeholders on an independent review by an appointed actuary of the adequacy of their reserves.
- d) Consent – KAFS should ensure that it has clear and informed consent from the data subjects through the data controllers (insurance companies) when and where required.

3.6. Additionally, due regard should be given to the provisions of the Data Protection Act, 2019 and the data protection principles when processing data.

Safeguards and Security of Data

- 3.7. In order to prevent unauthorized access of data, KAFS will implement robust access controls and mechanisms.
- 3.8. Where necessary, routine backups and recoveries will be set up to ensure availability and protection of data.
- 3.9. The data protection officer should regularly monitor access to data to detect and promptly respond to any incident or potential security incident.
- 3.10. Where KAFS intends to share any data with third parties, this should be done in compliance with the data protection Act, 2019.
- 3.11. The data protection officer should also ensure that data sharing agreements are duly signed with all third parties to whom data is being shared with and from whom data has been received.

Personal Data Relating to Health

- 3.12. Personal data relating to the health of a data subject may only be processed by or under the responsibility of a health care provider or by a person subject to the obligation of professional secrecy under any law

Rectification or Erasure

- 3.13. Where data is no longer in use or required, the data protection officer shall oversee the secure disposal of such data using the appropriate methods based on the sensitivity of the data.

Notification & Communication of Breach

- 3.14. Where personal data has been accessed or acquired by an unauthorized person, and there is a real risk of harm to the data subject whose personal data has been subjected to unauthorized access, a Data protection officer shall:
 - a) Assess the impact of the breach on all parties involved;
 - b) Notify the office of the Data Protection Commissioner and the affected data subjects within 72 hours; and

- c) Recommend and implement corrective actions aimed at preventing any future breaches.

Training and Awareness

- 3.15. KAFS will provide regular training sessions on data protection and data management to its employees.

General Penalty

- 3.16. According to the Data Protection Act, 2019, a person who commits an offence under the Act for which no specific penalty is provided or who otherwise contravenes the Act shall, on conviction, be liable to a fine not exceeding **THREE MILLION SHILLINGS** or to an **IMPRISONMENT** term not **EXCEEDING TWO YEARS** or to **BOTH**.
- 3.17. In addition to any penalty, the court may order the forfeiture of any equipment, or any article used or connected in any way with the commission of an offence or order or prohibit the doing of any act to stop a continuing contravention.

Enforcement

- 3.18. This policy shall come into force from the date of the Board's approval, or any other date as directed by the Board.
- 3.19. Non-compliance with this policy may lead to strict disciplinary action including termination of contractual or employment terms.

4 GOVERNANCE FRAMEWORK

- 4.1. To ensure effective implementation of the Policy, all personnel at all levels need to understand their roles and responsibilities.

Responsibility for the Success of the Policy

- 4.2. An effective Data Protection Policy is one in which all staff, consultants and directors are free to speak up on instances of breach (or potential breach) of professional or ethical standards.
- 4.3. It is the responsibility of all KAFS employees, consultants and directors to adhere to this Policy if they come across, or suspect, malpractice, wrongdoing or risk in the undertaking of all actuarial work at KAFS.

Board of Directors

- 4.4. Ensure that Management designs effective programs that ensure protection of data.

Management

- 4.5. The Management has the overall responsibility for this Policy, and for reviewing the effectiveness of actions taken in response to any issues raised under the provisions of this Policy. Management has the overall responsibility for the design and implementation of a program which includes:
- a) Setting the tone at the top for the rest of the organization;
 - b) Develop, review and maintain this Policy;
 - c) Identifying the need for and providing training to parties who may deal with raised concerns;
 - d) Ensuring implementation of the Policy in the organization;
 - e) Reporting to the Board on what actions have been taken on the effectiveness of the Program.
 - f) Plan and carry out training and awareness programs for the employees on data protection and management
- 4.6. The Management shall hold records of all concerns and the handling of each and will report to the Chief Actuary if need be.

Employees

- 4.7. All employees are responsible for ensuring the users of data are aware of the existing data Protection policy at the onset of the project.
- 4.8. The employees must:
- a) Familiarize and adhere to this Policy;
 - b) Be alert to actual and potential breaches to professional and ethical standards; and
 - c) Report breaches of this policy and any associated procedures to the management.

Disciplinary Committee

- 4.9. There shall be a disciplinary committee which shall be responsible for managing all breaches of this code of conduct in compliance with the company's due processes and enforce disciplinary actions.
- 4.10. The committee shall comprise of:
- a) A Senior Management Representative (Chairperson)
 - b) The Head of Actuarial Practice or an Appointed Senior Actuary
 - c) A Human Resources Representative
 - d) Any other independent member deemed necessary
- 4.11. The committee shall:
- a) Review and assess the severity of any reported breaches;
 - b) Oversee that the investigations are carried out in a fair and impartial manner
 - c) Determine the appropriate disciplinary actions based on the severity of the violation
 - d) Conduct hearings and allow the accused members an opportunity for defense

5 APPROVAL

Thus, opted and signed by the management and Chief Actuary of KAFS in January 2025.

APPROVED BY

Ezekiel Macharia

Chief Actuary & Managing Director – Kenbright Actuarial and Financial Services Limited

Date: January 2025

Signed: 

About Us

Kenbright Actuarial & Financial Services (KAFS)
Prism Towers, 26th Floor
3rd Ngong Avenue, Nairobi
Kenya
www.kenbright.co.ke

Customer Service Lines: +254 (020) 22 111 52

Document Version

January 2025

Version 1.0: Creation

Reproduction – in total or in part – only with the permission of KAFS.

Key Contacts

E Macharia, FIA C.Act, FeASK
Chief Actuary & Managing Director
E-mail: ezekiel@kenbright.africa
Phone: +254 722 540 045