CAPITAL MARKETS AUTHORITY

DATA PROTECTION POLICY

August 2023

Contents

Abbreviations

AU- African Union

CMA- Capital Markets Authority

COK- Constitution Of Kenya

DPA- Data Protection Act

DPIA- Data Protection Impact Assessment

DPO- Data Protection Officer

EU – European Union

ODPC- Office of the Data Protection Commissioner

Preface

The Authority recognizes that in this digital age data has become valuable. The Authority generates, collects, stores and transfers data daily. Data generated can range from personal information, financial records, sensitive personal data, and intellectual property. As the reliance on data grows, so does the need to protect it from unauthorized access, misuse, and breaches.

The Constitution of Kenya guarantees the right to privacy as a fundamental right. To give effect to this constitutional right under Article 31 (c) and (d), Kenya enacted a comprehensive data protection legislation in 2019 (The Data Protection Act,2019) hereinafter referred to as the ACT which mirrors the EU General Data Protection Regulation(GDPR).

Our commitment to data protection goes beyond compliance with the law. Data breaches can have severe consequences, not only for our staff and stakeholders but also impact our reputation as a trusted securities regulator. Therefore, we have developed a robust data protection policy and stringent security protocols which include continuous staff training to ensure that data is handled responsibly and securely throughout its lifecycle.

Data protection is a collective responsibility that involves the Board of Directors, Senior Management, Staff and other stakeholders. By fostering a culture of data protection and promoting best practices, we can ensure the security and privacy of sensitive information in a rapidly evolving digital world.

Finally, I wish to to reaffirm the Authority's commitment to data protection. It is not just a legal requirement but an integral part of our core values as an organization. We will continue to invest in the latest technologies, stringent processes, and a culture of data protection to protect the data entrusted to us.

Ugas S. Mohamed
Chairman,
Capital Markets Authority

Foreword

In today's digital age, information is more than just data. It represents our personal lives, our business decisions, and our aspirations. As our world becomes increasingly interconnected, the importance of ensuring that this information remains private, secure, and processed with integrity cannot be overstated.

In today's interconnected world, where data plays a pivotal role in shaping businesses and driving innovation, we recognize that trust as one of the foundations to our success.

This Data Protection Policy embodies our commitment to uphold this trust. It is a testament to the steps we take, the technologies we deploy, and the culture we foster to protect the data we are entrusted with. We believe that, by being transparent and proactive in our approach to data protection, we can pave the way for a more secure, responsible, and trusted digital environment.

In the rapidly evolving landscape of digital technology and regulations, we pledge to remain vigilant, agile, and uncompromising in our mission to safeguard personal data.

As we embark on this journey of data protection, every employee is expected to embrace and internalize this policy. We will collectively build a culture that respects privacy and nurtures an environment of trust.
I encourage all stakeholders, to familiarize themselves with the details of this Data Protection Policy. Together, we will not only comply with the law but also set new benchmarks in data protection.

Thank you for entrusting the Authority with your data. We take this responsibility seriously and promise to go above and beyond to safeguard your privacy while striving to earn and retain your trust every step of the way.

FCPA Wyckliffe Shamiah
Chief Executive Officer
Capital Markets Authority

Preamble

Policy Background

Data protection refers to the processing of personal data which is collected and entered in a record, by or for a data controller or processor, by making use of automated or nonautomated means. Further, data protection encompasses individual privacy on information related to a person (hereinafter referred to as ***the data subject***). It is the fair and proper use of information about people, clients, stakeholders, suppliers amongst others within one's ecosystem. The growth of digital technology has made the generation, transmission and storage of data exponentially increase, and hence posing more challenges to the right to privacy.

Privacy is a fundamental human right, enshrined in numerous international human rights instruments including Article 29 of the Universal Declaration of Human Rights which has been domesticated by Governments across the globe. Data protection dates to 1948 when the **Universal Declaration of Human Rights (UDHR)** declared in Article 12 that: "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks".* The right to privacy is also enshrined in international legal instruments such as The International Covenant on Civil and Political Rights [(ICCPR) and the UN Convention on the Right of the Child.

Data protection is regulated globally, regionally, and nationally through conventions, laws and policies. International Instruments include General Data Protection Regulations (GDPR), **EU Charter of Fundamental Rights,** Council of Europe Convention and the Malabo Convention (AU).

The right to privacy in Kenya was in 2019 highlighted and recognised by the **enactment of the Data Protection Act of 2019** which was assented into law on 8 November 2019 and commenced effective 25 November 2019. The Act gives effect to Article 31(c) and (d) of the Constitution and establishes the Office of the **Data Protection** Commissioner. The following national Instruments provide for the right to privacy namely:

i. The Constitution of Kenya 2010,
ii. Data Protection Act,2019 and attendant regulations,
iii. Access to Information Act: and
iv. Computer Misuse and Cyber Crimes Act, 2018.

The Act also assigns the subject certain rights and requires responsibility by persons and legal persons who record and use personal information.

Policy and Legal Framework

This policy shall at all times comply with the following:

i. Constitution of Kenya 2010;

ii. Data Protection Act, 2019;

iii. Access to Information Act, 2019;

iv. Data Protection General Regulations, 2021;

v. Archives Act,1990;

vi. Capital Markets Act as amended; and

vii. other relevant legal instruments.

1. Policy Statement

This policy stipulates the management of Personal Data and the commitment of the Capital Markets Authority to protect Personal Data of all its data subjects in Kenya and abroad.

2. Purpose

The purpose of the data Protection Policy is to provide a framework for the collection and processing of personal data by the Authority and the implementation of the DPA. Towards compliance of the DPA, the Authority should ensure adherence to the highlights of the DPA namely:

a) Fair and proper use of personal data collected and processed by the Authority.
b) The purpose of data collection should be relevant to its use.
c) Data should be protected against loss and unauthorized access.
d) Subjects should have the right to know what data is collected about him or her.
e) Subjects should have the right to access any data related to him or her.
f) Subjects should be able to challenge the retention of data or amend or erase data about him or her.

3. Scope

This Policy applies to all personal data collected and held by the Authority in relation to relevant subjects such as the Board, employees, and relevant stakeholders both in Kenya and abroad.

4. Definitions

"Authority" Capital Markets Authority.

"**anonymization**" means the removal of personal identifiers from personal data so that the data subject is no longer identifiable.

"**biometric data**" means personal data resulting from specific technical processing based on physical, physiological or behavioral characterization including blood typing, fingerprinting, deoxyribonucleic acid analysis, earlobe geometry, retinal scanning and voice recognition;

"**Cabinet Secretary**" means the Cabinet Secretary responsible for matters relating to information, communication, and technology.

"**consent**" means any manifestation of express, unequivocal, fee, 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 Commissioner**" means the person appointed under section 6 of the Data Protection Act.

"**Data controller**" means a natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purpose and means of processing personal data.

"**Data processor**" means a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the data controller.

"**Data protection focal point**" means the most senior Authority personnel who assists the data controller in carrying out its, his or her responsibilities regarding this Policy.

"**Data protection impact assessment**" means a tool and process for assessing the protection impacts on data subjects in processing their personal data and for identifying remedial actions as necessary to avoid or minimize such impacts.

"**Data Protection Officer**" means an Authority personnel who supervises, monitors and reports on compliance with the Data Protection Act and this Policy.

"**data subject**" means an identified or identifiable natural person who is the subject of personal data.

"**encryption**" means the process of converting the content of any readable data using technical means into a coded form.

"**Filing system**" means any structured set of personal data which is readily accessible by reference to a data subject or according to specific criteria, whether centralised, decentralised, or dispersed on a functional or geographical basis.

"**health data**" means data related to the state of physical or mental health of the data subject and includes records regarding the past, present, or future state of the health, data collected during registration for, or provision of health services, or data which associates the data subject to the provision of specific health services.

"**identifiable natural person"** means 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.

"IOSCO" means the International Organisation of Securities Commissions.

"**office**" means the office of the Data Protection Commissioner

"**National security organs**" has the meaning assigned to it under Article 239 of the Constitution

"**person**" has the meaning assigned to it under Article 260 of the Constitution;

"**personal data**" means any information relating to an identified or identifiable natural person;

"personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

"**processing"** means any operation or sets of operation 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, adaption or alteration
c) Retrieval, consultation or use;
d) Disclosure by transmission, dissemination, or otherwise making available; or alignment or combination, restriction, erasure or destruction; or

e) Alignment or combination, restriction, erasure or destruction.

"profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's race, sex, pregnancy, marital status, health status, ethnic social origin, colour, age, disability, religion, conscience, belief, culture, dress, language or birth; personal preferences, interests, behavior, location or movements;

"**pseudonymization**" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, and such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable natural person;

"**register"** means the register kept and maintained by the Data Commissioner under section 21;

"**restriction of processing**" means the marking of stored personal data with the aim of limiting their processing in the future;

"**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; and

"**third Party**" means natural or legal person, public authority, agency or other body, other than the data subject, data controller, data processor or persons who, under the authority of the data controller or data processor, are authorised to process personal data including IOSCO EMMOU signatory members states as the case may be;

5. Types of Personal Data Collected

Depending on the nature of our interaction with individuals and the services we provide, we may collect and hold the following types of personal data:

a. **Identity Data** - This includes first name, last name, username or similar identifier, marital status, title, date of birth, and gender.
b. **Contact Data** - This covers billing address, delivery address, email address, and telephone numbers.
c. **Financial Data** - This incorporates bank account and payment card details.
d. **Transaction Data** - This includes details about payments and other details of products and services from us.
e. **Technical Data** - This covers internet protocol (IP) address, login data, browser type and version, time zone setting and location, browser plug-in types and

versions, operating system and platform, and other technology on the devices you use to access our platform.

f. **Profile Data** - This consists of usernames and passwords, purchases or orders made by you, your interests, preferences, feedback, and survey responses.
g. **Usage Data** - Information about how you use our website, products, and services.
h. **Marketing and Communications Data** - Your preferences in receiving marketing from us and third parties and your communication preferences.
i. **Sensitive Personal Data** We may also collect, store, and use the following special categories of more sensitive personal information:

- Racial or ethnic origin.
- Religious or philosophical beliefs.
- Trade union membership.
- Genetic and biometric data.
- Data concerning health.
- Data concerning a natural person's sexual orientation.

6. Principles of Data Protection

There are seven (7) Principles of data protection in Kenya. The seven (7) principles are drawn from the **EU General Data Protection Regulation (GDPR), 2016.** The principles are:

a) Lawful and Fair Processing; this refers to the ethical and legal principles that organizations must adhere to when collecting, processing, handling, and disclosing personal information of individuals. All processing of personal data should be lawful and fair. It should be transparent to individuals that personal data concerning them are collected or otherwise processed and to what extent the personal data is or will be processed.

b) Purpose Specification: Personal data needs to be collected for specified, explicit and legitimate purposes and should not be processed in a way incompatible with those purposes.

c) Data minimization: Data collected shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

d) Accuracy: Personal data should be recorded as accurately as possible and where necessary, updated to ensure it fulfils the purpose(s) for which it is collected.

e) Storage and Limitation- Data relating to a data subject must be deleted, archived or anonymized once it has served its purpose.

f) Integrity and Confidentiality- Personal data must be 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 and using appropriate technical or organisational measures.

g) **Accountability-** the data controller is responsible for and must demonstrate compliance with the principles of Data Protection.

7. Data Protection Officer

The Authority, being a data controller and data processor, shall appoint or designate a data protection officer (hereinafter referred to as DPO). The DPO shall; -

a) advise the Authority, employees and stakeholders on the data processing requirements provided under this Act or any other written law.
b) inform and advise the Authority and the employees who carry out processing of their obligations pursuant to this Act.
c) ensure on behalf of the Authority that this Act is complied with.
d) facilitate capacity building of employees involved in data processing operations.
e) provide advice on the Data Protection Impact Assessments (DPIAs), monitor its performance if required, and co-operate with the Commissioner with regard to the performance of the DPIA.
f) co-operate with the Data Commissioner and any other authority on matters relating to the protection of personal data.
g) be the contact point for the data subjects and the Data Protection Commissioner.
h) ensure the Authority responds to requests from data subjects exercising their rights under the Act.
i) be involved in the monitoring and evaluation of the systems that process and manage personal data at the Authority.
j) And any other function as required by the Act.

8. Duty to Notify

The Authority, before collecting personal data the Authority shall inform the data subject of:

a) The rights of data subject specified under section 26 of the Data Protection Act.
b) The fact that the Authority is collecting personal data and the purpose for which the personal data is being collected.
c) The third parties whose personal data has been or will be transferred to, including details of safeguards adopted where applicable.
d) The contacts of the data controller or data processor and on whether any other entity may receive the collected personal data.
e) A description of the technical and organizational security measures taken to ensure the integrity and confidentiality of personal data.

f) The data being collected pursuant to any law and whether such collection is voluntary or mandatory.
g) The consequences, if any, where the data subject fails to provide all or any part of the requested data.
h) A notification by the Authority to the Data Commissioner of a data breach.

9. Lawful and Fair Processing of Personal Data

When processing personal data, the Authority will ensure that:

a) there is an appropriate legal basis or legitimate interests clearly connected to the specific purpose of the processing of personal data such as consent, contract, legal obligation or in the exercise of authority.
b) the data subject is granted the highest degree of autonomy possible with respect to control over their personal data.
c) the data subject knows what they consented to and there is an easy means to withdraw consent.
d) restricting processing where the legal basis or legitimate interests ceases to apply.
e) the processing of personal data is done in a fair manner and does not adversely affect the rights and freedoms of the data subject.
f) Tohe Authority shall not process personal data unless the data subject consents to processing for one or more specified purposes.

10. Minimization of Collection

At the point of data collection, the Authority will ensure the following elements are implemented.

a) The Authority will limit the amount of personal data collected to what is necessary for the purpose.
b) The Authority shall demonstrate the relevance of the data to the processing in question.
c) The personal data shall be Pseudonymized as soon as it is no longer necessary to have directly identifiable personal data removed.
d) anonymizing or deleting personal data where the data is no longer necessary for the purpose.
e) making data flows efficient to avoid the creation of more copies or entry points for data collection than is necessary, and the application of available and suitable technologies for data avoidance and minimization.

11. Accuracy of data

The Authority shall ensure that the data collected is accurate. The elements necessary to implement the principle of data accuracy shall include the following but not limited to:

a) ensuring data sources are reliable;
b) recording personal data particulars accurately;
c) verification of the correctness of personal data with the data subject before and at different stages of the processing depending on the nature of the personal data, in relation to how often it may change.
d) erasing or rectifying inaccurate data without delay.
e) mitigating the effect of an accumulated error in the processing chain.
f) giving data subjects an overview and easy access to personal data in order to control accuracy and rectify as needed.
g) the use of technological and organizational design features to decrease inaccuracy.

12. Safeguard and Security of Personal Data

The Authority shall safeguard personal data to ensure privacy, protect the right of the data subjects and maintain trust. This shall include but not limited to the following:

a) **Access Controls**: Only authorized individuals shall have access to personal data. This will be managed with authentication and authorization.
b) **Firewalls and Intrusion Detection Systems**: to prevent unauthorized external access to networks and systems.
c) **Physical Security** such as locking servers in a secure room, can also be important, especially for very sensitive data.
d) **Data Breach Response Plan**: Incliding identifying and closing the security hole, notifying affected users, and potentially notifying the relevant authorities.
e) **Anonymization and Pseudonymization**: Involving replacing identifiers in the dataset so that the individuals to whom the data belong can't be directly identified. Pseudonymization is a method where personally identifiable information fields within a data record are replaced by one or more artificial identifiers, or pseudonyms. Anonymization is the process of removing personally identifiable information from data sets, so that the individuals whom the data describe remain anonymous.
f) **Data Minimization**: Only collect the minimum amount of personal data needed for the specific purpose.
g) **Employees Training**: Ensuring that all employees are trained in data protection and understand the importance of their role in maintaining privacy.

h) **Regular Audits and Updates**: Regular checks on systems and processes to ensure they are functioning as intended. Keeping systems and software updated is also critical to ensure that vulnerabilities are patched.

i) **Encryption**: This is a technique to convert data into a code to prevent unauthorized access. Data in transit and at rest should be encrypted to protect from interception or breaches.

13. Consent

a) The Authority shall obtain express consent from the Data Subject prior to processing personal data and sensitive personal data

b) The processing of personal data shall be for the specific purposes for which consent was given.

c) Where a new purpose is required, the Authority shall first notify and obtain a subsequent express consent of the data subject.

d) In taking a data subject through the consent form the following shall be explained to the data subject:

i. **Purpose of Data Collection**. -The Authority shall clearly state the purpose for which data is being collected, ensuring it is specific, explicit, and legitimate.

ii. **Voluntary Consent-**Data subjects' consent will be given freely without any coercion, and they will have the option to withdraw consent at any time without any adverse consequences. Where lack of consent will prevent the Authority from providing services to the data subject, this shall be stated.

iii. **Informed Consent-**The Authority shall provide clear and easily understandable information about the data processing activities, including the types of data collected, the purposes, the data recipients and the data retention periods.

iv. **Opt-In Mechanism-** Consent will be obtained through appropriate means including a signature, ticking of boxes or using of the words "YES" or "NO".

v. **Age Verification-** If the data processing involves individuals under the age of consent, the Authority shall obtain parental or guardian consent.

vi. **Separate Consents -**Separate consents will be obtained for different processing activities, ensuring that the data subjects can give granular consent for each purpose.

vii. **Right to Withdraw Consent-**Data subjects will be informed of their right to withdraw consent at any time and the process to do so will be clearly explained.

viii. **Revoking Consent-**The Authority shall notify data subjects of the possibility to revoke their consent, and the withdrawal will be acknowledged and acted upon promptly.

ix. **Conditional Services-**The Authority will not condition the provision of services or benefits on the data subject's consent to processing that is unnecessary for the performance of the service.

x. **Notification of Changes-** In case of any changes to the data processing that may affect the original consent, data subjects will be notified and asked for renewed consent if necessary.

xi. **Recordkeeping-**The Authority shall maintain records of all obtained consents, including the time, date, and method of obtaining consent.

xii. **Data Subject's Rights -**Data subjects shall be informed of their data protection rights, including the right to access, rectify, erase, restrict processing, and data portability.

xiii. **Language and Presentation -**The consent provisions will be presented in clear and straightforward language, avoiding legalese or technical jargon.

xiv. **Data Protection Officer (DPO)-**Data subjects will be provided with the contact details of the Data Protection Officer (DPO) to address any concerns or inquiries regarding their data.

e) There shall be a regular audit and verification on the accuracy and completeness of consent records.

f) There shall be a periodic review and update of consent practices to align with changes in data processing activities or regulations.

g) The policy acknowledges that there will be exceptional circumstances where personal data can be processed without the data subjects consent. There may be limitations on data subject rights when required by the law or when there are competing rights and therefore it will require an assessment based on the facts and circumstances.

14. Data Protection Impact Assessment (DPIA)

DPIA is a systematic process used to identify and assess the potential risks and impacts of a data processing activity on individuals' privacy and data protection rights. Where a processing operation is likely to result in high risk to the rights and freedoms of a data subject, by virtue of its nature, scope, context, and purposes the Authority shall, prior to the processing, carry out a data protection impact assessment. The Data Protection Impact Assessment shall be carried out in accordance with the Data Protection Act and the regulations and guidelines issued thereunder.

15. Reporting concerns and Non-Compliance

Below is the procedure for reporting any data concerns or non-compliance:

a) Every employee has a responsibility to promptly report any data protection concerns or instances of non-compliance that come to their attention. This includes issues related to data handling, security breaches, unauthorized access, or any other data protection-related matter.
b) All employees are encouraged to report any concerns related to data protection or instances of non-compliance with the data protection policy immediately upon noticing the non-compliance to their immediate supervisor in writing.
c) The supervisor shall report all concerns or non-compliance reports to the Data Protection Officer immediately upon detection or notification but not later than twenty-four hours of notification or detection.
d) All reports made will be treated with confidentiality and protection. Whistleblowers will be shielded from retaliation, and their identities will be kept confidential.
e) The Authority shall provide an option for anonymous reporting to encourage employees who may be hesitant to report concerns openly.
f) All reports, investigations, and actions taken to address concerns and non-compliance will be documented and maintained in a secure and confidential manner.
g) Employees who report concerns will receive feedback on the status and outcome of the investigation, to the extent allowed by applicable laws and regulations.

16. Processing and Transferring Personal Data Out of Kenya

The Authority in executing its mandate may transfer personal data to external third parties in other countries. Before transfer, the Authority shall:

a) Give sufficient proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of personal data ;

b) Ensure that the required degree of protection is afforded to personal data under the laws of that country. The third party service providers to whom a data transfer is made should have appropriate safeguards in place to protect personal data;

c) Ensure that the processing of sensitive personal data out of Kenya shall only be effected upon obtaining consent of the concerned data subject;

d) Before conducting international data transfers, the Authority may conduct a data transfer impact assessment to evaluate the risks associated with the transfer and implement necessary measures to ensure data protection; and

e) The processing of sensitive personal data out of Kenya shall be effected upon approval by the Data Commissioner.

17. Data Breach Management

Below is the procedure for handling a data breach;

a) Employees are required to notify the DPO as soon as possible upon becoming aware of a data breach and to properly record the breach.

b) The Authority shall without undue delay and, where feasible, not later than 72 (seventy-two) hours after having become aware of it, notify the Office of the Data Commissioner of the breach of personal data.

c) The Authority in its capacity as a data processor shall notify the data controller within 48 Hours of the breach.

d) The notification referred above shall at least:

   i. describe the nature of the personal data breach.

   ii. description of the measures taken by the data controller to address the data breach.

   iii. recommendation on the measures to be taken by the data subject to mitigate the adverse effects of the security compromise.

   iv. where applicable the identity of the unauthorized person who may have accessed or acquired the personal data; and

   v. the name and contact of the data protection officer.

e) If a personal data breach is likely to result in personal injury or harm to a data subject, the Authority shall within a reasonable time notify the data subject in writing of the data breach and take mitigating measures as appropriate without undue delay. In such cases, the data controller should also notify the Data Protection Officer of the personal data breach.

f) The data controller shall maintain a data breach register recording the facts relating to the breach, its effects and the remedial action taken.

18. Training and Awareness

The Authority shall conduct a training session to senior management and employees to equip them with the necessary skill to handle personal data responsibly. On onboarding, new employees shall be sensitized on data protection requirements depending on their role. There shall be regular awareness initiatives such as lunch box sessions, on-the-job learning, mentorship and webinars organized by the DPO in liaison with the Learning and Development team. Employees will have unlimited access to the relevant learning materials.

19. Data Partners

The Authority may engage data partners to process data on its behalf or on execution of its mandate. The Authority shall ensure that the required degree of protection is afforded to personal data. The Authority will ensure that third party service providers to whom a data transfer is made has appropriate safeguards in place to protect personal data.

20. Roles and Responsibilities

The implementation framework outlines the hierarchy and responsible departments, committees, sections, units and individuals facilitating and overseeing the implementing this Policy is as follows:

a) **Board of the Capital Markets Authority**

b) The role of the Board will be:

i. To approve the Policy once presented by management; and

ii. Recommending to the National Treasury and Economic Planning to consider and forward the Policy to the Public Service Commission for final approval.

c) **Chief Executive Officer**

The role of the Chief Executive Officer will be to:

i. Appoint a Data Protection Officer.

ii. Appoint the Data Protection Committee.

iii. Approve resources for Data Protection activities

iv. Oversee compliance with the provisions of the Data Protection Act, 2019

d) **Role of the Data Protection Officer**

The role of the Data Protection Officer will be as outlined under clause 7 of this policy.

e) **Role of the Data Protection Committee**

The Committee shall:

i. participate in the development and review of the Authority's Data Protection Policy;

ii. ensure sensitization of the Board and employees and relevant stakeholders of the Authority;

iii. support the implementation of and reinforce commitment to the Data Protection Policy;

iv. monitor and advise relevant parties on changes on the legal framework on data protection in Kenya; and

v. monitor and evaluate the implementation of this policy.

f) **Heads of directorates/ departments and divisions/ units**

They will be required to ensure compliance with Data Protection Act, 2019 and General Regulations 2021 in their day-to-day operations.

g) **Employees**

They will be required to:

i. Fully comply with the provisions of the Data Protection Act , 2019 and General Regulations 2021;
ii. Participate in capacity building and sensitization sessions when called upon;
iii. Report any data protection breach as provided for.

21. Data Retention

The Authority will be committed to ensuring compliance with data retention inline with the provisions of the Data Protection Act and any other related legislations. In particular**;**

a) Personal data that is not recorded in individual case files is not to be retained longer than necessary for the purposes for which it is collected.
b) All individual case files, whether open or closed, are considered permanent records and must be retained in accordance with the Public Archives Act.
c) Where specific legislations guide on data retention the provisions shall apply

22. Monitoring and Compliance

The Data Protection Officer will continuously monitor the implementation of this policy. The Data Protection Committee will assist the Data Protection Officer to conduct periodic evaluation with a view to assessing the relevance, efficiency, effectiveness, impact and sustainability of the provisions of this policy.

23. Policy Review

This policy will be reviewed every three (3) years or when need arises.

This Policy comes into effect on this ……12th…… day of ……Oct… 2023.

CHIEF EXECUTIVE OFFICER **BOARD CHAIRMAN**