

Data Protection Policy and Procedures

Renaissance Securities (Nigeria) Limited

RenCap Securities (Nigeria) Limited

RC Asset Management Limited

Policy owner

Nicholas Okonkwo

Approved by

The Board

Samuel Sule



Approved: Feb 2026

Effective by

August 2020

Proposed Next revision date

July 2024 (if material changes are required)

Version no

1

Date

August 2020

Author

Nicholas Okonkwo

Main Changes

2	31 July 2023	Nicholas Okonkwo	Changes in Governing legislation and body
3	September 2024	Nicholas Okonkwo	General Review
4	January 2025	Nicholas Okonkwo	General Review
5	January 2026	Nicholas Okonkwo	Inclusion of RC Asset Management

Contents

1.	Introduction	4
1.1.	The purpose of this document.....	4
1.2.	Background and Legislation.....	4
1.3.	Overview, Scope and Governance.....	5
1.4.	NDPA Sections	6
1.5.	Procedure ownership and change management	6
1.6.	Key definitions	6
2.	Processing of Personal Data	8
2.1.	Information to the Data Subject	8
2.2.	Lawful Processing	9
2.3.	Data Minimization	10
2.4.	Accuracy	10
2.5.	Storage Limitation	10
2.6.	Procuring Consent	10
2.7.	Data Privacy Policy.....	10
2.8.	Security and Confidentiality.....	11
2.9.	Protecting the Rights of Data Subject	11
2.10.	Sensitive Personal Data	12
2.11.	Processing Personal Data for Marketing Purposes.....	12
2.12.	Transfer of Personal Data	13
	(a) Third Party Transfers	13
	(b) Foreign Transfer.....	13
	(c) Inter-Company transfers	13
3.	Data Protection Measures.....	14
3.1.	Technical and Organizational Measures.....	14
3.2.	Responsibility in Processing.....	15
4.	Data Protection Officer	15
5.	Data Protection Impact Assessment (DPIA).....	16
6.	Personal Data Breach.....	16
6.1.	Reporting a Personal Data Breach.....	16
7.	Training and Awareness.....	16
8.	Audits	17
9.	Contact.....	17
	Appendix 1	18
	RENAISSANCE NIGERIA PRIVACY POLICY	18
	1. Introduction	18

2.	Applicable Law	18
3.	What Personal data do we Collect from You?.....	18
4.	Governing Principles.....	19
5.	Why do we collect personal data from you?	19
6.	We use this information because:.....	20
7.	How Do We Collect Your Personal data?	20
8.	With Whom Does Renaissance Nigeria Share Your Information?	21
9.	Does Renaissance Nigeria Transfer Your Information to Third Countries?	21
10.	Data Retention	21
11.	Your Rights	22
12.	How do we ensure protection of your personal data?.....	22
13.	Policy Violation	22
14.	Policy Updates	22
15.	How to Contact Us	22

1. Introduction

1.1. The purpose of this document

The implementation of the Nigeria Data Protection Act on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, (“NDPA”) becomes effective on 14 June 2023 imposing changes designed to increase the level of accountability for organisations processing personal data and includes greater transparency for individuals and the limitation of the permitted use of personal data.

The Policy highlights the conduct expected of Renaissance Securities (Nigeria) Limited, RenCap Securities (Nigeria) Limited, RC Asset Management Limited and any other entity within the group (together referred to as “Renaissance Nigeria” or the “Firm”), its officers and employees and third parties acting on its behalf while processing personal data.

This Policy sets out principles relating to the protection of any information relating to an identified or identifiable natural person (“data subject”) that can be identified, directly or indirectly, in particular 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 identity of that natural person (“personal data”).

This Policy describes how personal data must be collected, processed, transferred and stored to meet the Firm’s data protection standards and to comply with the relevant applicable laws.

This Policy highlights and /or ensures that Renaissance Nigeria:

- Complies with the NDPA;
- Protects the rights of its employees, customers and contractors;
- Is transparent for individuals into how and why it stores and processes individuals’ personal data;
- Protects itself from the risks of a data breach.

Other areas of focus include the following:

- Accountability, including appointment of Data Protection Officer (DPO) or Unit Skills of the DPO should include:
 - Understanding of the operations processing involved;
 - Understanding of IT and Data Security;
 - Knowledge of the business sectors.
- Data Safeguards insuring NDPA requirements are built into the Firm’s technical and organisational arrangements;
- Increase employee awareness including amongst the other obligations to report data breaches to the relevant Data Protection Authority within 72 hours and to notify individuals without undue delay if there is a high risk of harm;
- Periodic Internal Audits on the existing Data Protection arrangements;
- Ongoing monitoring to ensure protection, security and confidentiality of data and to identify and address threats to security and integrity of data;
- Ensuring third-party service providers adhere to the NDPA requirements and the Firm’s security standards and policies;
- Ensures compliance with any other legal and regulatory requirements; and
- Ensuring the privacy by design concept is implemented accordingly.

1.2. Background and Legislation

The Constitution of the Federal Republic of Nigeria 1999 (as amended) in section 37 guarantees the privacy of citizens' homes correspondence, telephone conversations, and telegraphic communications. The enforcement of the constitutional right of privacy is the sole responsibility of the National Assembly.

Pursuant to the NDPA, the Nigerian Data Protection Commission was established to perform among others, the function of creating guidelines to govern the exchange of data and information.

Following the Global Data Protection Regulation in the EU adopted on 14 April 2016 and effective on 25 May 2018 and the urgent need to have a data protection legislation encapsulating the various pocket data protection laws, Nigeria through the National Assembly released the Nigeria Data Protection Act (NDPA) 2023 to serve as a body of regulations that set guidelines for monitoring and enforcing the privacy of citizens personal data.

The NDPA 2023 is the current legislation governing the control and processing of personal data within Nigeria of natural persons residing, domiciled, or ordinarily operating in Nigeria or residing, domiciled, or ordinarily operating outside Nigeria but of Nigerian descent.

1.3. Overview, Scope and Governance

This policy has been developed for Renaissance Nigeria and is applicable to the processing of Personal Data by Companies and third parties who process Personal Data on behalf of Renaissance Nigeria. Specifically, this policy applies to:

- (a) Any and all personal data processed in Nigeria by or on behalf of Renaissance Nigeria, including employees, customers, contractors, local stakeholders, external consultants, business partners and suppliers' personal data, whether or not such personal data is processed by automated means;
- (b) Any and all personal data processed in Nigeria by or on behalf of Renaissance Nigeria and transferred outside Nigeria, including employees, customers, contractors, local stakeholders, external consultants, business partners and suppliers' personal data.

This policy does not apply to Data rendered anonymous. Data are rendered anonymous if individual persons are no longer identifiable, either directly or indirectly.

This Policy has been prepared in accordance with (the "NDPA").

There are six major principles for processing personal data including:

- Lawful, fair and transparent processing;
 - Purpose of requesting certain personal data;
 - Data minimization;
 - Data Accuracy;
 - Storage Limitation;
 - Integrity and confidentiality.
- (c) The policy ensures:
- that data is collected and processed in accordance with the specific and lawful purpose agreed and/ or consented to by the Data Subject;
 - the right of the Data Subject to the accuracy and adequacy of the data; and
 - that data is stored for a specified period and adequately secured.

This Policy may be supplemented or amended by additional policies and guidelines from time to time. Enforcement date commences on August 1 2020.

1.4. NDPA Sections

The NDPA is divided into 12 parts with 66 sections outlined below:

- Part 1: The Objectives and Application
- Part 2: Establishment of the Nigeria Data Protection Commission, and its Governing Council
- Part 3: Appointment of the National Commissioner for the Commission
- Part 4: Financial Provisions
- Part 5: Principles and Lawful basis Governing Processing of Personal Data
- Part 6: Rights of Data Subject
- Part 7: Data Security
- Part 8: Cross Border Transfer of Personal Data
- Part 9: Registration and Fees
- Part 10: Enforcement
- Part 11: Legal Proceedings
- Part 12: Miscellaneous Provisions

1.5. Procedure ownership and change management

Any proposed material changes to this policy or associated procedures must be raised to Compliance. Upon approval by Compliance the changes will be fed into the main body of the policy for final sign-off.

1.6. Key definitions

Consent	of the Data Subject means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, through a statement or a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her.
Data Subject	means any natural person, who can be identified, directly or indirectly, in particular 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 identity of that natural person; It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as

	but not limited to MAC address, IP address, IMEI number, IMSI number, SIM, Personal Identifiable Information and others
Data Controller	means a natural or legal person who either alone, jointly with other persons or in common with other persons or a statutory body which determines the purposes for, and the way Personal Data is processed or is to be processed. In the context of this Policy, “Data Controller” refers to Renaissance Nigeria.
Data Protection Compliance Organization (DPCO)	means any entity duly licensed by NITDA for the purpose of training, auditing, consulting, and rendering services and products for the purpose of compliance with this Regulation or any foreign Data Protection Law or Regulation having effect in Nigeria.
Data Protection Impact Assessment	means the assessment of the impact of a processing operation on the protection of Personal Data (hereafter “DPIA”)
Data Protection Officer	means an individual appointed by the Data Controller and has the responsibilities set out in section 4 of this policy
Inter-Company Transfer	refers to the transfer of data between Renaissance Nigeria, and other entities within the Renaissance Capital Africa Group.
Personal Data	means any information relating to Data Subject.
Personal Data Breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data. This includes breaches that are the result of both accidental and deliberate causes.
Personal Identifiable Information (PII)	means information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in a context.
Processing	means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as • collection, • recording, • organisation, • structuring, • storage, • adaptation or alteration, • retrieval, • consultation, • use, • disclosure by transmission, • dissemination or otherwise making available, • alignment or combination, • restriction, • erasure or destruction.

Relevant Authorities	means The Nigeria Data Protection Commission or any other statutory body or establishment having government's mandate to deal solely or partly with matters relating to Personal Data.
Sensitive Personal Data	means data relating to • religious or other beliefs, • sexual orientation, • health, • race, • ethnicity, • political views, • trades union membership, • criminal records or any other sensitive personal information.
Third Party	means a natural or legal person, which processes Personal Data on behalf of the Data Controller.

2. Processing of Personal Data

Renaissance Nigeria Personnel or any Third Party acting on its behalf shall comply with the following principles when processing Personal Data:

2.1. Information to the Data Subject

For the purposes of this Policy, the relevant controllers are:

Controller entity:	Contact details
Renaissance Securities (Nigeria) Limited	The Wings Office Complex 6th Floor, East Tower 17A Ozumba Mbadiwe Avenue Victoria Island, Lagos Tel: +234 (1) 448-5324
RenCap Securities (Nigeria) Limited	The Wings Office Complex 6th Floor, East Tower 17A Ozumba Mbadiwe Avenue Victoria Island, Lagos Tel: +234 (1) 448-5324

The Firm's email for the Data Protection enquiries: compliance@rencapafrica.com

The Firm's affiliates which from time to time act as data processors shall not engage another processor without prior specific or general written authorization of the controller.

We obtain your personal data when you provide it to us via email, telephone or by any other means.

We collect your personal data in the ordinary course of our business relationship including managing your transactions.

The categories of personal data that we may process, subject to applicable laws, are as followed:

- Personal details (name, surname, gender, date of birth, national identification number, passport number, bank verification number, tax identification number, images of passports, driving licenses and signatures, credentials (login and password details);
- Family details (names and contact details of family members and dependents – HR related);
- Contact details (address, telephone number(s), email address);
- Employment details (role, names of current and former employers, work address, work telephone number, work email address, work-related social media profile details);
- Financial details (billing address, bank account numbers, transaction details, portfolio details).

Renaissance Nigeria may also obtain information, including personal data and sensitive personal data, about your directors, employees, officers, agents, or clients. We and you will each treat as confidential (both during and after the termination of the relationship between us and you) any information learned about each other, our or your investment strategy or holdings or products or services in the course of the relationship pursuant to these terms and, except as otherwise agreed, shall not disclose the same to any third party without the other party's consent.

2.2. Lawful Processing

Renaissance Nigeria Personnel shall ensure that Processing is based on at least one of the following legal bases:

- (a) *Consent*: The Individual has given their consent to the processing of their Personal Data for one or more specific purposes. In addition,
- Renaissance Nigeria shall be able to demonstrate that the Individual has consented to processing of their Personal Data, and
 - Prior to giving consent, the Individual shall be informed of their right to withdraw their consent at any time. At consent's withdrawal – which shall be as easy as giving consent – the processing must cease.

In summary, Consent must be unambiguous, freely given, specific and informed. Therefore, Consent obtained under duress or on the basis of misleading information will not be a valid legal basis for Processing. Consent cannot be inferred from non-response to a communication. For special categories of Personal Data, explicit written consent of Data Subjects must be obtained unless an alternative legal basis for Processing exists.

- (b) *Contract*: Processing is necessary for:
- the performance of a contract to which the Data Subject is party; or
 - entering into a contract at the request of the Data Subject only.
- (c) *Legal obligation*: Processing is necessary for compliance with a legal obligation to which Renaissance Nigeria or its affiliate is subject to including carrying out money laundering or conflict checks, and for fraud and financial crime prevention purposes;
- (d) To pursue legitimate interests, in particular in the course of the operational support and development of our businesses, including to evaluate customer service, efficiency and cost, and for risk management purposes;
- (e) for reporting (including, without limitation, transaction reporting and position reporting) to, and audits by, national and international regulatory, enforcement or exchange bodies;

- (f) for complying with court orders associated with us or any Affiliate
- (g) *Vital interest*: Processing is necessary in order to protect the vital interests of the Individual or of another natural person;
- (h) *Public interest*: Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in Renaissance Nigeria
- (i) *Proper Motives*: Renaissance Nigeria shall not seek consent that may engender direct or indirect propagation of atrocities, hate, child rights violation, criminal acts and anti-social conducts;

2.3. Data Minimization

Data Minimization means that only Personal Data needed to fulfil the purpose for which it is collected should be processed. The Personal Data that are being processed need to be:

- Adequate (enough data);
- Relevant (necessary to fulfil the purpose);
- Limited to and not more than needed to fulfil the purpose.

2.4. Accuracy

The Personal Data processed within Renaissance Nigeria needs to be accurate and up to date. Data should not be kept unless it is reasonable to assume that it is accurate. In order to achieve optimal accuracy (quality) of the Personal Data, Renaissance Nigeria shall, as far as possible, obtain Personal Data from the Data Subject directly.

2.5. Storage Limitation

Personal Data must not be retained any longer than is necessary for the purposes for which they are processed and in compliance with applicable legal requirements with respect to document retention. The Personal Data must be destroyed, with traceable record, or archived after the retention period when they are no longer necessary for the Processing activity.

2.6. Procuring Consent

The following guiding principles are applicable for procuring consent from Data Subjects for the purpose of obtaining and processing their Personal Data in line with section 2.2(a) of this Policy:

- Renaissance Nigeria will only collect Personal Data after disclosing the purpose of collection to the Data Subject. Furthermore, Renaissance Nigeria will not process Personal Data in a manner that is incompatible with the originally stated purposes.
- Renaissance Nigeria will only obtain consent from Data Subjects who have the legal capacity to do so.
- Renaissance Nigeria will only obtain consent in a manner that is without fraud, coercion, or undue influence. The request for consent shall be presented in an intelligible and easily accessible form, using clear and plain language.
- Renaissance Nigeria should be able to demonstrate to the Relevant Authorities at all times that consent has been obtained from Data Subjects for the processing of their personal data.
- Renaissance Nigeria shall obtain consent where Personal Data may be transferred to a Third Party.

2.7. Data Privacy Policy

For every Personal Data collected, a Privacy Policy specific to the data being collected shall be documented in a written form and displayed on the medium through which the Data is obtained. The Privacy Policy shall be

simple, conspicuous and easily understood by the class of Data Subject targeted. Furthermore, the Data Subject will be required to read and provide verifiable consent to Renaissance Nigeria for obtaining and processing their Personal Data.

These mediums include the following:

- Electronic forms (including web forms, electronic documents)
- Emails
- Paper-based forms
- Web tokens

The Privacy Policy shall address the following:

- What constitutes the Data Subject's consent;
- Specification of Personal Data being collected where this has not been explicitly defined in the medium being used (e.g. through named fields in forms);
- Purpose of collection of Personal Data;
- Methods used to collect, store and process the personal data;
- Access by third parties and the purpose of such access;
- Available remedies in the event of violation of the privacy policy
- The time frame for the remedy
- Renaissance Nigeria's commitment to ensuring protection of the Personal Data

Renaissance Nigeria's data privacy policy is contained in *Appendix 1*.

2.8. Security and Confidentiality

Renaissance Nigeria will take reasonable precautions to secure Personal Data against accidental or unlawful destruction or loss, alteration, unauthorized disclosure or access. These precautions include technical, physical and organizational security measures to prevent unauthorized access.

2.9. Protecting the Rights of Data Subject

Data Subjects have rights when it comes to Renaissance Nigeria's handling of their Personal Data. Those rights include:

- the right to request access to their Personal Data. This right is exercisable where the request is reasonable and permitted by extant laws or regulations. Renaissance Nigeria shall provide reasonable and accessible means for Data Subject to submit their requests, which do not have to take any specific form and can be submitted by any method.

Renaissance Nigeria shall take appropriate measures to provide the requested information in writing, through electronic means or orally, in line with request of the Data Subject, provided that the identity of the Data Subject has been verified. Renaissance Nigeria shall provide such information free of charge except where it has been demonstrated that the requests are unfounded and excessive. In the event of unfounded and excessive request by the Data Subjects, Renaissance Nigeria may either charge a reasonable fee for the administrative costs or write a letter to the Data Subject stating refusal to act on the request and copy the Relevant Authorities on every such occasion.

Where Renaissance Nigeria has reasonable doubts concerning an Data Subject making the request, Renaissance Nigeria may request the provision of additional information necessary to confirm the identity of the Data Subject. Within 30 days of validating the identity of any Data Subject submitting a request for access to their Personal Data, Renaissance Nigeria shall provide the requested information, or provide legitimate reasons for not complying with their request.

- the right to request that Renaissance Nigeria erase their Personal Data if it is no longer valid or necessary for the purposes for which it was collected or if it is incomplete or inaccurate. Renaissance Nigeria shall delete such Personal Data based on request from the Data Subject and shall take reasonable steps to notify all Third Parties to delete such Personal Data.
- the right to rectify or amend inaccurate or incomplete Personal Data.
- the right to withdraw their Consent at any time.
- the right to object to Renaissance Nigeria's processing of their Personal Data if there are compelling legitimate grounds to do so and to the extent permitted by law or regulation. Data Subject have the right to object to Renaissance Nigeria's processing of their Personal Data for direct marketing purposes.
- the right to obtain restriction of Renaissance Nigeria's processing of their Personal Data if one of the following applies:
 - i. the accuracy of the Personal Data is contested,
 - ii. the processing is unlawful,
 - iii. the Controller no longer needs the Personal Data for the purposes of processing, and
 - iv. the Data Subject has objected to the processing as set out above.
- the right to receive their Personal Data in a commonly used and machine-readable format and the right to transmit these data to another Data Controller when the processing is based on (explicit) consent or when the processing is necessary for the performance of a contract.

2.10. Sensitive Personal Data

Renaissance Nigeria Personnel shall not process Sensitive Personal Data unless one of the following legal bases is met:

- The Data Subject has given explicit consent to the data processing;
- processing is carried out by a non-profit body with political, philosophical, religious or trade union purposes in the course of its legitimate activities and only relates to its (former) members or to persons who have regular contact with it for such purposes;
- processing concerns data explicitly made public by the Data Subject;
- processing is necessary:
 - to carry out the obligations of, and to exercise the specific rights of, Renaissance Nigeria or of the Data Subject in the employment
 - to protect the vital interests of the Data Subject or another natural person (when the Data Subject cannot give consent);
 - to establish, exercise or defend legal claims or when courts act in their judicial capacity;
 - for preventative or occupational medicine purposes: "for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services law or pursuant to contract with a health professional";
 - for public interest reasons in the area of public health;
 - for substantial public interest reasons; or
 - for the detection or prevention of crime or fraud to the extent permitted by applicable Laws;

2.11. Processing Personal Data for Marketing Purposes

Renaissance Nigeria Personnel will not process Personal Data for the purposes of direct marketing, unless the individual gave a valid consent and effective procedures are implemented allowing Individuals to withdraw their

consent at any time.

2.12. Transfer of Personal Data

Renaissance Nigeria shall transfer and store Personal Data to entities within the group of companies and third parties on Renaissance Nigeria's behalf within and outside Nigeria for legitimate business activities in accordance with Data Protection Laws and professional standards.

(a) Third Party Transfers

Renaissance Nigeria will ensure that any transfer of Personal Data to a Third Party is governed by written agreements with third parties that impose obligations that reflect the requirements of the NDPA and this Policy.

(b) Foreign Transfer

Renaissance Nigeria shall not transfer Personal Data to another country or organization outside Nigeria unless the Company is satisfied that the Personal Data is adequately protected in accordance with extant Data Protection Laws and Regulations. Renaissance Nigeria shall rely on the decision of the Relevant Authorities in determining which countries or foreign jurisdictions have implemented adequate safeguards for the protection of Personal Data. Where there is no decision by the Relevant Authorities, Renaissance Nigeria may transfer Personal Data to a foreign country, provided any of the following conditions are met:

- i. that the Data Subject has explicitly consented to the proposed transfer, having been informed of the possible risks of such transfers;
- ii. the transfer is necessary for the performance of a contract between the Data Subject and the Controller or the implementation of pre-contractual measures taken at the Data Subject's request;
- iii. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Controller and another natural or legal person;
- iv. the transfer is necessary for important reasons of public interest;
- v. the transfer is necessary for the establishment, exercise or defence of legal claims; and
- vi. the transfer is necessary 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; Provided, in all circumstances, that the Data Subject has been manifestly made to understand through clear warnings of the specific principle(s) of data protection that are likely to be violated in the event of transfer to a third country, this proviso shall not apply to any instance where the Data Subject is answerable in duly established legal action for any civil or criminal claim in a third country.

(c) Inter-Company transfers

Renaissance Nigeria may disclose personal data to other entities within Renaissance Capital Africa Group of companies, for legitimate business purposes in accordance with applicable Laws and ensuring data safety, integrity, and segregation of access permissions.

Transfers of Personal Data to other entities within the Renaissance Capital Africa Group will be subject to the terms of this Policy. This also includes the storage or processing of Personal Data on information systems that can be accessed by other entities within the Renaissance Capital Africa Group. All entities within the Renaissance Capital Africa Group should be signatories to an inter-company agreement that includes contractual terms to ensure the protection of the Personal Data being transferred in accordance with the terms of this Policy.

3. Data Protection Measures

Renaissance Nigeria shall implement appropriate measures to ensure and to be able to demonstrate that processing of Personal Data is performed in accordance with extant Data Protection Laws and Regulations, taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity of the rights and freedoms of the individuals.

3.1. Technical and Organizational Measures

The following technical and organizational measures will be in place:

(a) Encryption

Implement encryption techniques on all categories of electronic Personal Data including data at rest and data in transit in order to restrict ability to comprehend such data to authorized personnel only.

(b) Physical Access Control

Ensure that all infrastructure and facilities housing Personal Data both in electronic and non-electronic formats are protected with adequate physical access controls in order to minimize the risk of unauthorized access.

(c) Logical Access Control

Implement logical access controls including configuration of access rules, identification and strong authentication mechanisms over information systems hosting Personal Data in order to restrict access to authorized individuals only.

(d) Data Retention Policy

Develop and implement a data retention policy which would ensure that Personal Data are not retained for longer than necessary in order to reduce the likelihood and/or severity of a data breach.

(e) Incident Management

Implement an effective process which ensures adequate detection and response to incidents and security breaches that may expose Personal Data.

(f) Human Resource Security

Implement measures to reduce the risk of Renaissance Nigeria personnel breaching data protection regulations. These measures will be in place prior to staff employment (e.g. through adequate background checks), during employment (e.g. through effective end user information security awareness programs) and post-employment (through appropriate deactivation process).

(g) Endpoint Protection

Implement endpoint protection solution on all workstations and servers including anti-malware solutions in order to minimize the possibility of a breach of Personal Data.

(h) Backup and Recovery

Perform regular backup of data stored in servers and workstation to ensure availability of Personal Data.

(i) Network Security

Minimize the risk of breach to Personal Data through network and connectivity channels. This is achieved through adequate network access controls, network segmentation, firewall, intrusion prevention and detection, SSL protocol, flow encryption, strong authentication, etc.

(j) **Security of Non-Electronic Media**

Reduce the risks of unauthorized access to physical documents containing Personal Data through appropriate document classification, securing printing equipment, clear desk policies, amongst other measures

3.2. Responsibility in Processing

Renaissance Nigeria shall ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. The processor shall take all measures to ensure security of Personal Data processing.

The processor shall notify the Controller without undue delay after becoming aware of a personal data breach.

The notification shall:

- (a) Describe the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned, and the categories and approximate number of Personal Data records concerned;
- (b) Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- (c) Describe the likely consequences of the Personal Data breach; and
- (d) Describe the measures taken or proposed to be taken by the Controller to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Data Protection Officer

Renaissance Nigeria shall appoint a DPO who shall among others, have the specific responsibilities of:

- (a) ensuring that the Data Controller and any individual or organization responsible for processing the data are aware of and performs its obligations under this policy as well as the extant data protection laws;
- (b) act as contact to Data Subject making enquiries or exercising their right as it relates to the processing of their data;
- (c) monitoring compliance of Renaissance Nigeria with this policy as well as other data privacy instruments;
- (d) provide advice and recommendations to Renaissance Nigeria on the interpretation and application of data protection rules;
- (e) raising awareness on data protection issues as well as ensuring that the employees of Renaissance Nigeria at all levels are adequately trained;
- (f) oversee and advise on the performance of a DPIA;
- (g) report on failures to comply with this policy to senior management;
- (h) liaise with the DPCO in the performance of the annual external audits; and
- (i) cooperate with any data protection supervisory authority as well as act as a point of contact on issues pertaining to data processing.

The DPO shall report directly to the highest level of senior management only and must be allowed to operate independently with the full support of senior management. It is expected that the DPO shall be adequately trained annually in the performance of his/her responsibilities. Failure to do so shall be a breach of this policy.

Renaissance Nigeria reserves the right to outsource data protection functions to a verifiable competent individual or firm.

5. Data Protection Impact Assessment (DPIA)

Renaissance Nigeria shall perform periodic DPIAs in order to identify, analyse and mitigate the risks associated with processing Personal Data. These risks include unlawful processing as well as any compromise of the confidentiality, integrity, and accuracy of such data.

In addition to the periodic DPIAs, an assessment would be necessary prior to any of the following events:

- The introduction of a new processing technology.
- Significant changes to business processes and technology solutions that have touchpoints with Personal Data.
- Where Renaissance Nigeria intends to collect a new type of Personal Data in order to perform business operations.
- Whenever the Relevant Authorities issue a list of processing operations for which a DPIA is required.
- Where Personal Data will be transferred to a Third Party or a foreign country.

The Assessment shall cover the following:

- a description of the envisaged processing operations and the purposes of the processing
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes
- an assessment of the risks to the rights and freedoms of data subjects
- Description of measures to mitigate the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data and to demonstrate compliance with this Regulation.

Renaissance Nigeria shall consult the Relevant Authorities before starting the processing operation, if it appears that the processing will result in a high risk for the rights of individuals and no effective measures are in place to mitigate the risk.

6. Personal Data Breach

6.1. Reporting a Personal Data Breach

- i. All Renaissance Nigeria Personnel who suspect or become aware of a Data Breach including situations where the Data relates to information on computers or electronic device or system will immediately report it to the Data Protection Officer.
- ii. Where Personal Data is involved, Renaissance Nigeria Personnel should immediately report it through compliance@rencapafrika.com and will not attempt to investigate any suspected/proven breach themselves, nor discuss the case with any third parties, unless they receive a sign-off from both the Legal and the Compliance Department.
- iii. Renaissance Nigeria shall maintain a Personal Data Breach Register. Any Personal Data Breach will be recorded in the Personal Data Breach Register.

7. Training and Awareness

Renaissance Nigeria shall on a biennial basis conduct mandatory data protection training and periodic privacy awareness communications to all Renaissance Nigeria Personnel. Records of training attendance will be maintained and monitored. These training programs will include an assessment test to evaluate understanding of the Data Protection Policy. Non-completion of this mandatory training and assessment test within the defined

timelines will amount to a breach of this Policy.

8. Audits

In line with the NDPA, where Renaissance Nigeria processes more than 1000 Data Subjects for a period of six (6) months or 2000 Data Subjects for a period of twelve (12) months, it shall appoint a DPCO to conduct external data privacy audit and file same for the firm. The audit shall aim to achieve the following:

- (a) assess Renaissance Nigeria level of compliance with the NDPA;
- (b) evaluate compliance with the firm's own data protection policy;
- (c) identify potential gaps and weaknesses in firm's processes; and
- (d) give requisite advice and/or remedial actions for identified gaps.

This external audit shall be carried out on an annual basis failing which shall constitute a breach of this policy.

9. Contact

Any questions regarding this Policy or Renaissance Nigeria Personnel rights and obligations can be addressed to the DPO at: compliancelagos@rencap.com.

Appendix 1

RENAISSANCE NIGERIA PRIVACY POLICY

1. Introduction

Renaissance Securities (Nigeria) Limited and RenCap Securities (Nigeria) Limited (together referred to as “Renaissance Nigeria”) understands the importance of privacy when collecting and or processing your (“data subject”) personal information and your right to object to, consent to or withdraw consent to processing your personal information. Accordingly, we have described in this policy our practices related to the use, storage, and disclosure of personal information we collect from or about you when you interact with us in the course of our providing/receiving services to/from you, including when you use our website. This Privacy Policy also describes our processing of the personal data of individuals representing our business customers and service providers.

2. Applicable Law

This Privacy Policy is prepared in line with the Nigeria Data Protection Act 2023 (“NDPA”).

3. What Personal data do we Collect from You?

The NDPA defines personal data as “any information relating to an identified or identifiable natural person (‘Data Subject’).

It further defines an identifiable natural person as “one who can be identified, directly or indirectly, in particular 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 identity of that natural person”.

More specifically, we may collect:

- (a) Contact Information: Your name, home address, phone number, name of next of kin, or the phone number of your next of kin, national identity number, international passport number, drivers’ license number.
- (b) Financial Information: This includes any information we may require such as your bank account number, bank verification number, bank branch, account name; or to enhance payment such as credit and debit card type, billing address, etc.
- (c) Demographic information and interests: Depending on whether you are our employee, a contract staff, a recruitment candidate, service provider/vendor, website visitor or customer, we may collect from you information that describes your demographic or behavioral characteristics such as your date of birth, age, gender, IP address, geographic location (e.g. postcode/zip code), etc. We use such information for improving the quality of our service offerings to customer, or, in respect of our employees, contract staff, recruitment candidates etc. for record purposes.
- (d) Sensitive personal data: Sensitive personal data is data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trades union membership, criminal records or any other sensitive personal information. We will usually not request sensitive personal information from you; however, in the unlikely event that it becomes necessary for the purpose of our business, we will seek your express consent before processing your sensitive personal data.
- (e) By providing any personal information that is or could be sensitive personal information, you agree that you have given us your consent to collect, store, use, and transfer this personal information for the purposes for which it was provided and otherwise in accordance with the terms of this Privacy Policy.
- (f) In addition, we may enter into contracts with third parties who may process certain sensitive personal data

such as your medical history, etc. However, we will ensure that such third parties are mandated to seek your consent prior to processing such sensitive personal data.

- (g) Voice data: This includes recordings of your voice or conversations you have with people. We store recordings of calls placed to our Sales/Origination teams, and Traders to take necessary instructions and for quality assurance purposes. By keeping recordings of your calls, we are able to review the contents of the calls to analyze our performance, determine best practices, and resolve any compliance issues that may arise. However, we only retain these recordings for a period of seven (7) years after which they are deleted.

4. Governing Principles

In processing the different forms of your personal data described above, we are guided by the governing principles stipulated in Part 4-6 of the NDPA. These principles are summarized below:

- (a) Your personal data will be collected and processed in accordance with specific, legitimate and lawful purpose consented to by you;
- (b) Your personal data will be adequate, accurate and without prejudice to the dignity of human person;

Processing your Personal Data

- (c) Your personal data will be stored only for the period within which it is reasonably required;
- (d) Your personal data secured against all foreseeable hazards and breaches such as theft, cyberattack, viral attack, dissemination, manipulations of any kind, damage by rain, fire or exposure to other natural elements.
- (e) Your consent shall be sought before processing your personal data. "Consent" means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, through a statement or a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her.

5. Why do we collect personal data from you?

Personal data collected from you is used to:

- provide you (our customers) with our various service offerings;
- receive your payment, make any refunds or credits and send any confirmations;
- send you service communications, such as letters, emails, telephone calls and website contents;
- in the case of recruitment candidates, effectively communicate with you and provide you with regular updates relating to the recruitment process.
- manage and administer our services and business, including performing our record-keeping requirements;
- maintain the operational availability and reliability of our IT systems with infrastructure backups and testing (which may use a copy of live data where test data is not practical);
- confirm your identity and to prevent fraud;
- improve our products and services, including through statistical analysis and research for program development;
- send you marketing communications, offers, and invitations to events, which may be based on our segmentation and modelling of your personal information;
- provide you with assistance in an emergency, including communicating with your emergency contacts;
- share with authorized government agencies and as otherwise described below.
- in the case of calls to our Call Centre, maintain quality control and operational efficiency.

6. We use this information because:

(a) Our Customers:

- it is necessary to enter into and perform our contract with you to provide the agreed contractual services to you;
- we have a legitimate business interest in assisting you with the agreed contractual services;
- you have provided your consent at the point of collection;
- we have a legitimate business interest in improving and promoting our service and better understanding of how customers use it;
- we have a legitimate business interest in ensuring that our technical systems operate properly;
- you have provided your consent at the point of collection (in the case of information that we use to send you marketing communications);
- we have a legitimate interest in ensuring customer satisfaction and regulatory compliance.

(b) Our Employees, Contract Staff and Service Providers

- we have a legitimate business interest in ensuring proper records of all our employees, staff, and service providers are kept.
- we have a legitimate business interest in managing our business and protecting it from fraud.

(c) Recruitment Candidates

- we have a legitimate interest in managing the recruitment exercise effectively for the purpose of our business.
- it is necessary for compliance with legal obligations regarding qualifications of candidates.
- we have a legitimate interest in ensuring that we constantly communicate with you throughout the recruitment process.

(d) Our Website users:

- you have provided your consent at the point of collection;
- we have a legitimate business interest in assisting you with our services;
- you have provided your consent at the point of collection (in the case of information that we use to send you marketing communications);
- we have a legitimate interest in ensuring customer satisfaction and regulatory compliance

7. How Do We Collect Your Personal data?

We collect personal data:

- By making formal requests to employees and contract staff;
- Through emails to recruitment candidates and customers;
- Through our e-service platforms to customers;
- By recording calls you make to our Sales/Origination teams, and Traders.
- Through web forms on our website;
- Through technical methods such as the use of cookies.

8. With Whom Does Renaissance Nigeria Share Your Information?

We typically do not transfer your personal data to third parties; however, in the exceptional cases listed below, we may disclose your data to third parties. However, we will ensure that, as stipulated in the NDPA, such third party does not have a history of violating data protection principles. In addition, we enforce data protection principles in our written contracts with third parties who have access to your data.

Below are circumstances where we may transfer your data to third parties, to:

- process your information on our behalf, or to assist us in providing our services such as: third party agencies for the recruitment of employees and contract staff, third-party processors of customer data, medical clinics for providing health care services to employees and contract staff.
- those acting on your behalf. Where local regulations require, we may obtain your consent in writing for the purpose of allowing someone else to act on your behalf.
- banks, financial firms and payment services for the purposes of processing payments.
- government agencies and authorities, law enforcement officials, law courts, or to third parties:
 - if we believe disclosure is required by applicable law, regulation or legal process (such as pursuant to a subpoena or judicial order as well as statutory filings to regulators); or
- to protect and defend our rights, or the rights or the rights, health, or safety of third parties, including to establish, make, or defend against legal claims; or
 - in the interest of public health and safety.
- persons providing services to Renaissance Nigeria, including its professional advisers (e.g. auditors, lawyers, and technical consultants).
- persons with whom we may discuss selling any part of our business or to whom we sell any part of our business.

9. Does Renaissance Nigeria Transfer Your Information to Third Countries?

We store and process your personal information on our computers in Nigeria but may need to transfer your data to other entities within Renaissance Capital Africa Group in different countries in furtherance of the contractual or proposed contractual relationship between us. In such cases, the country will have an adequate data protection law or mitigating data security controls in place. We will seek your consent where we need to send your data to a country without an adequate data protection law.

For the avoidance of doubt, transfers of personal data will be carried out in accordance with Part VIII of the NDPA.

Whether stored in the country or abroad, we protect your information using physical, technical, and administrative security measures to reduce the risks of loss, misuse, unauthorized access, disclosure and alteration.

10. Data Retention

We store your information for as long as legally required or for so long as necessary to support our business and consistent with our record retention policies. In general, this storage will be:

- at least for the duration of our relationship,
- for as long as you can bring a claim against us and for us to be able to defend ourselves, and
- for any period required by tax and other applicable laws and regulations.
- in the case of voice data, for seven (7) years after placing a call to our Sales/Origination teams, and Traders.

11. Your Rights

You have rights when it comes to our handling of your personal data. Those rights include the right to:

- request for access to your personal data where those requests are reasonable and permitted by law or regulation. We shall provide reasonable and accessible means for you to submit your requests, which do not have to take any specific form and can be submitted by any method.
- request that we erase your personal data if it is no longer valid or necessary for the purposes for which it was collected or if it is incomplete or inaccurate.
- rectify or amend inaccurate or incomplete personal data. If you believe that any data we hold about you is incorrect or incomplete, you may contact our Data Protection Officer for options on how to correct/complete such data.
- withdraw your consent at any time. This can be initiated by contacting our Data Protection Officer.
- object to our processing of your personal data if there are compelling legitimate grounds to do so and to the extent permitted by law or regulation. You have the right to object to our processing of your personal data for direct marketing purposes.
- receive your personal data in a commonly used and machine-readable format and the right to transmit these data to another data controller when the processing is based on (explicit) consent or when the processing is necessary for the performance of a contract.
- lodge a complaint with the NDPC where you believe our processing of your data violates the requirements of the NDPA.

12. How do we ensure protection of your personal data?

We use appropriate measures and safeguards (including physical access controls and secure software and operating environments) to keep your Personal Data confidential and secure. These safeguards are regularly reviewed to protect against unauthorized access, disclosure, and improper use of your information, and to maintain the accuracy and integrity of that data. Do note, however, that these protections do not apply to information you choose to share in public areas such as third-party social networks.

Personal Data Breach Notification: Renaissance Nigeria will inform relevant authorities and if necessary affected individuals of personal data breach within 72 hours of being aware of the breach, where Personal Breach refers to a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

13. Policy Violation

In the event of any violation of this policy, we will remediate the issue within 7 calendar days.

14. Policy Updates

If we change the way we handle your Personal Data, we will update this Notice. We reserve the right to make changes to our practices and this Notice at any time, please check back frequently to see any updates or changes to our Notice.

15. How to Contact Us

If you have any questions or comments regarding this Privacy Policy or any complaints about our adherence to it, please contact **compliance@rencapafrika.com** or contact our Customer Care Center by telephone or post. We will then respond in accordance with our policies.