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 Regulation 2019 ("NDPR") made pursuant to the National Information Technology Development Agency Act, 2007.

3. What Personal data do we Collect from You?

The NDPR 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 2 of the NDPR. 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 NDPR, 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 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 Article 2.11 and 2.12 of the NDPR.

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 NITDA where you believe our processing of your data violates the requirements of the NDPR.

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 **compliancelagos@rencap.com** on **Tel +234 (1) 448-5324 x5385** or contact our Customer Care Center by telephone or post. We will then respond in accordance with our policies.