Data Protection Polices and Procedure

FSDH Capital Limited
Data Protection Policies and Procedures

DOCUMENT CONTROL

Document Review History

Version	Creation/Modification Date	Purpose	Approved By
1.0	MARCH 2022	Initial Document	Board of Directors

Document Review Frequency

This document will be reviewed every three (3) years to incorporate emerging developments on the subject. However, where there are emerging regulatory issues that required amendment of the policy, the review period may be shortened.

Table of Contents

Mission Statement 5

Our vision 5

1.0 Policy Statement 6

2.0 Purpose 6

3.0 Scope 6

3.1 Definitions 7

3.2 Nigeria Data Protection Regulation (NDPR) 8

3.2.1 Personal Data 8

3.2.2 The NDPR Principles 9

3.3 Data Protection Officer 9

4.0 Objectives 10

5.0 Governance Procedures 11

5.1 Accountability & Compliance 11

5.1.1 Privacy by Design 12

5.1.2 Data Protection Audit 13

5.2 Legal Basis for Processing *(Lawfulness*) 13

5.2.1 Processing Special Category Data 14

5.3 Third-Party Processors 14

5.4 Data Retention & Disposal 15

6.0 Data Protection Impact Assessments (DPIA) 15

7.0 Data Subject Rights Procedures 16

7.1Consent & The Right to be Informed 16

7.1.1 Consent Controls 17

7.1.2 Information Provisions 18

7.2 Privacy Notice 19

7.3. Employee Personal Data 19

7.4 The Right of Access 19

7.5 Data Portability 20

7.6 Rectification & Erasure 20

7.6.1 Correcting Inaccurate or Incomplete Data 20

7.6.2 The Right to Erasure 21

7.7 The Right to Restrict Processing 21

7.8 Right to Objections 22
7.9 Right around Automated Decision Making 22
8.0 Oversight Procedures 23
8.1 Security & Breach Management 23
9.0 Transfers & Data Sharing 23
10.0 Audits & Monitoring 25
11.0 Training 26
12.0 Penalties 27

Mission Statement

We thrive to be responsible custodian of personal information of our customers, suppliers and employees. We are committed as required by regulation to ensure full compliance with the NDPR and GDPR.

Our vision

We aim to uphold the highest data governance standards at all times through professionalism, competence and expertise.

1.0 Policy Statement

FSDH Capital *(hereinafter referred to as the **"Company")*** needs to collect personal information to effectively carry out our everyday business functions and activities and to provide the products and services defined by our business type. Such data is collected from employees, customers, suppliers and clients and includes *(but is not limited to),* name, address, email address, data of birth, IP address, Bank Verification Numbers, private and confidential information and sensitive information.

In addition, we may be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations, however we are committed to processing all personal information in accordance with the **Nigerian Data Protection Regulation (NDPR) and General Data Protection Regulation (GDPR)**, and any other relevant data protection laws and codes of conduct *(herein collectively referred to as **"the data protection laws")**.*

The Company has developed this policy, procedures, controls and measures to ensure maximum and continued compliance with the data protection laws and principles, including staff training, audit measures and assessments. Ensuring and maintaining the security and confidentiality of personal and/or special category data is one of our top priorities and we are proud to operate a ***'Privacy by Design'*** approach, assessing changes and their impact from the start and designing systems and processes to protect personal information at the core of our business.

2.0 Purpose

The purpose of this policy is to ensure that the Company meets its legal, statutory and regulatory requirements under the data protection laws and to ensure that all personal and special category information is processed compliantly and, in the individuals, best interest.

The data protection laws include provisions that promote accountability and governance and as such the Company is committed to put comprehensive and effective governance measures into place to meet these provisions. The aim of such measures is to ultimately minimize the risk of breaches and uphold the protection of personal data. This policy also serves as a reference document for employees and third-parties on the responsibilities of handling and accessing personal data and data subject requests.

3.0 Scope

This policy applies to all staff within the Company *(*meaning permanent, and temporary staff, any third-party representatives or sub-contractors, volunteers, interns and agents engaged with the Company*).* Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

3.1 Definitions

"Biometric data" means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

"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, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

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

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

"Data protection laws" means for the purposes of this document, the collective description of the NDPR and GDPR and any other relevant data protection laws that the Company complies with.

"Data subject" means an individual who is the subject of personal data

"Data breach" Personal Data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted or destroyed, or otherwise processed.

"NDPR" means the *Nigeria Data Protection Regulation*

"GDPR" means the *General Data Protection Regulation (EU)*

"Genetic data" means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

"Personal data" means any information relating to an identified or identifiable natural person*('data subject'*); an identifiable natural person is 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.

"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.

"Sensitive data" means data relating to religious or other beliefs, sexually orientation, health, race, ethnicity, political views, trade union membership, criminal records, or any other sensitive personal information.

"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 toanalyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

"Recipient" means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with the law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

"Supervisory Authority" means an independent public authority which is established by the law

3.2 Nigeria Data Protection Regulation (NDPR)

The Nigeria Data Protection Regulation (NDPR) was issued in 2019. This was the first comprehensive and robust effort to regulate the data management sphere in Nigeria.

As the Company processes personal information regarding individuals (*data subjects*), we are obligated under the Nigeria Data Protection Regulation (NDPR) to protect such information, and to obtain, use, process, store and destroy it, only in compliance with its rules and principles.

3.2.1 Personal Data

Information protected under the NDPR is known as *"personal data"* and is defined as: –

"Any information relating to an identified or identifiable natural person; an identifiable natural person is 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."

The Company will ensure that a high level of care is afforded to personal data falling within the NDPR's **'special categories'** *(**sensitive personal data***), due to the assumption that this type of information could be used in a negative or discriminatory way and is of a sensitive, personal nature to the persons it relates to.

3.2.2 The NDPR Principles

Section 2 of the NDPR requires that personal data shall be: –

1. processed lawfully, fairly and in a transparent manner in relation to the data subject ***('lawfulness, fairness and transparency')***
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Section 2, not be considered to be incompatible with the initial purposes ***('purpose limitation')***
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ***('data minimisation')***
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ***('accuracy')***
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Section 2 subject to implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject ***('storage limitation')***
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ***('integrity and confidentiality').***

3.3 Data Protection Officer

Section 3 of the NDPR detail the obligations, requirements and responsibilities on firms to appoint a Data Protection Officer and specifies the duties that the officer themselves must perform.

A Data Protection Officer (DPO) must be appointed by a firm where: –

- The entity is a government organ, ministry, department, institution or agency
- The core activities of the controller/processor involve the processing of large set of Personal Data;
- The organisation processes Sensitive Personal Data in the regular course of its business

- The organisation processes critical national information infrastructureconsisting of Personal Data. 3.4.2
- Notwithstanding the above, an organisation may voluntarily appoint a DPO.

The DPO has the following major tasks:

- To inform and advise on NDPR/GDPR and related obligations;
- To monitor compliance with the NDPR/GDPR and related obligations (including awareness raising and training);
- To provide advice as regards data protection impact assessment and to monitor its performance;
- To cooperate with the supervisoryauthority;
- To act as the contact point for the supervisor authority.

4.0 Objectives

We are committed to ensuring that all personal data processed by the Company is done so in accordance with the data protection laws and its principles, along with any associated regulations and/or codes of conduct laid down by the Supervisory Authority and local law. We ensure the safe, secure, ethical and transparent processing of all personal data and have measures to enable data subjects to exercise their rights.

The Company has developed the below objectives to meet our data protection obligations and to ensure continued compliance with the legal and regulatory requirements.

The Company ensures that: –

- We protect the rights of individuals with regards to the processing of personal information.
- We develop, implement and maintain a data protection policy, procedure, audit plan and training program for compliance with the data protection laws.
- Every business practice, function and process carried out by the Company, is monitored for compliance with the data protection laws and its principles.
- Personal data is only processed where we have verified and met the lawfulness of processing requirements.
- We record consent at the time it is obtained and evidence such consent to the Supervisory Authority where requested.
- All employees are knowledgeable about their NDPR obligations and are provided with training in the data protection laws, principles, regulations and how they apply to their specific role in the Company.

- Individuals feel secure when providing us with personal information and know that it will be handled in accordance with their rights under the data protection laws.
- We monitor the Supervisory Authority, National Information Technology Development Agency (NITDA) for any NDPR news and updates, to stay abreast of changes, notifications and additional requirements.
- We have documented Data Breach controls for identifying, investigating, reviewing and reporting any breaches or complaints with regards to data protection.
- We have appointed a Data Protection Officer who takes responsibility for the overall supervision, implementation and ongoing compliance with the data protection laws.
- We have a dedicated Audit & Monitoring Program in place to perform regular checks and assessments on how the personal data we process is obtained, used, stored and shared. The audit program is reviewed against our data protection policies, procedures and the relevant regulations to ensure continued compliance.
- We store and destroy all personal information, in accordance with our retention policy and schedule which has been developed from the legal, regulatory and statutory requirements and suggested timeframes.
- Any information provided to an individual in relation to personal data held or used about them, will be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
- Employees are aware of their own rights under the data protection laws.

5.0 Governance Procedures

5.1 Accountability & Compliance

Due to the nature, scope, context and purposes of processing undertaken by the Company, our main governance objectives are to: –

- Educate senior management and employees about the requirements under the data protection laws and the possible impact of non-compliance
- Provide a dedicated and effective data protection training program for all employees
- Identify key stakeholders to support the data protection compliance program
- Allocate responsibility for data protection compliance champions and ensure that the designated person(s) has sufficient access, and support to perform the role

The technical and organisational measures that the Company has in place to ensure and demonstrate compliance with the data protection laws, regulations and codes of conduct, are detailed in this document and associated data governance framework and operationalization. The Company's sanction grid shall apply for the purpose of data governance implementation.

5.1.1 Privacy by Design

We operate a *'Privacy by Design'* approach and ethos, with the aim of mitigating the risks associated with processing personal data through prevention via our processes, systems and activities. We have developed controls and measures *(detailed below*), that help us enforce this ethos.

Data Minimisation

Under Section 2.2 of the NDPR, it advises that data should be *'limited to what is necessary'*, which forms the basis of our minimalist approach. We only obtain, retain, process and share the data that is essential for carrying out our services and/or meeting our legal obligations and only retain data for as long as is necessary.

Our systems, employees, processes and activities are designed to limit the collection of personal information to that which is directly relevant and necessary to accomplish the specified purpose. Data minimisation enables us to reduce data protection risks and breaches and supports our compliance with the data protection laws.

Measures to ensure that only the necessary data is collected includes: –

- Electronic collection*(i.e. forms, website, surveys etc*) only have the fields that are relevant to the purpose of collection and subsequent processing. We do not include*'optional'* fields, as optional denotes that it is not necessary to obtain
- Forms, contact pages and any documents used to collect personal information are to be reviewed yearly to ensure they are fit for purpose and only obtaining necessary personal information in relation to the legal basis being relied on and the purpose of processing

Restriction/Access Control

Our *Privacy by Design* approach means that we use Company-wide restriction methods for all personal data activities. Restricting access is built into the foundation of the Company's processes, systems and structure and ensures that only those with authorisation and/or a relevant purpose, have access to personal information. Special category data is restricted at all levels and can only be accessed by staff members who are obligated to perform processing as part of the customer service or development team.

Data Masking

In line with the CBN data security guideline, the Company has deployed Data Masking solution. Only data in test servers are masked. This is to ensure that when vendors are installing and testing solutions, they are unable to view Personally Identifiable Information (PII) data in the databases.

Hard Copy Data

Due to the nature of our business, it is sometimes essential for us to obtain, process and share personal and special category information which is sometimes available in a paper format. Where this is the case, we use a physical safe to store such documents.

5.1.2 Data Protection Audit

To enable the Company to fully prepare for and comply with the data protection laws, the internal Audit unit should carry out a Company-wide data protection audit to better enable us to record, categorise and protect the personal data that we hold and process.

The audit should identify, categorise and recorded all personal information obtained, processed and shared by our Company in our capacity as a controller/processor.

5.2 Legal Basis for Processing *(Lawfulness)*

At the core of all personal information processing activities undertaken by the Company, is the assurance and verification that we are complying with Section 2.2 of the NDPR and our lawfulness of processing obligations. Prior to carrying out any personal data processing activity, we identify and establish the legal basis for doing so and verify these against the regulation requirements to ensure we are using the most appropriate legal basis.

The legal basis is documented on our Privacy Notice and, where applicable, is provided to the data subject and Supervisory Authority as part of our information disclosure obligations. ***Data is only obtained, processed or stored when we have met the lawfulness of processing requirements, where: –***

- The data subject has given consent to the processing of their personal data for one or more specific purposes
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
- Processing is necessary for compliance with a legal obligation to which we are subject
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Company
- Processing is necessary for the purposes of the legitimate interests pursued by the Company or by a third party (*except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child).*

5.2.1 Processing Special Category Data

Special categories of Personal Data are defined in the data protection laws as: –

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation,explicit consent is required for the Processing of Sensitive Personal Data.

We will only ever process special category data where: –

- The data subject has given explicit consent to the processing of the personal
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law
- Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim
- Processing relates to personal data which are manifestly made public by the data subject
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- Processing is necessary for reasons of substantial public interest
- Processing is necessary for the purposes of preventive or occupational medicine, 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
- Processing is necessary for reasons of public interest in the area of public health

5.3 Third-Party Processors

The Companyutilizes external processors for certain processing activities *(where applicable*). ***Such external processing includes*** *(but is not limited to****): –***

- IT Systems and Services
- Legal Services
- Human Resources

Due diligence and Know Your Customer procedures and measures should be in place and review, assess and background check of all processors prior to forming a business relationship. We obtain documents, certifications, references and ensure that the processor is adequate, appropriate and effective for the task we are employing them for.

These parties are required to confirm and ensure compliance with the data protection regulations.

The continued protection of data subjects' rights and the security of their personal information is always our top priority when choosing a processor and we understand the importance of adequate and reliable outsourcing for processing activities as well as our continued obligations under the data protection laws for data processed and handled by a third-party.

We include data protection clauses in Service Level Agreements (SLAs) and contracts with each processor as per the services provided.

Processors are notified that they shall not share any client information or personal data of the Client and/or the Client's customers/clients with any third party except as required for the provision of the Service and to comply with the provisions of the Nigeria Data Protection Regulations (NDPR) 2019.

5.4 Data Retention & Disposal

The Company have defined procedures for adhering to the retention periods as set out by the relevant laws, contracts and our business requirements, as well as adhering to the NDPR requirement to only hold and process personal information for as long as is necessary. All personal data is disposed of in a way that protects the rights and privacy of data subjects *(e.g. shredding, disposal as confidential waste, secure electronic deletion, hard drive destruction) that*prioritises the protection of the personal data in all instances*.*

Please refer to our Archival policy.

6.0 Data Protection Impact Assessments (DPIA)

Individuals have an expectation that their privacy and confidentiality will be upheld and respected whilst their data is being stored and processed by the Company. We therefore utilise several measures and tools to reduce risks and breaches for general processing. However, where processing is likely to be high risk or cause significant impact to a data subject, we must utilise proportionate methods to map out and assess the impact ahead of time.

Where the Companyis considering carrying out processing that utilises new technologies, and/or where there is a likelihood that such processing could result in a high risk to the rights and freedoms of data subjects, it is necessary to carry out a Data Protection Impact Assessment (DPIA) *(sometimes referred to as a Privacy Impact Assessment*). A DPIA is not compulsory for all processing operations; however, it may be required for the following types of processing:

Pursuant to Section 3.2, we consider processing that is likely to result in a high risk to include: –

- Evaluation or scoring (profiling);
- Automated decision-making with legal or similar significant effect;
- Systematic monitoring;
- Sensitive Personal Data or Personal Data of a highly personal nature;
- When Personal Data Processing relates to vulnerable or differently data subjects;
- When considering the deployment of innovative processes or
- Application of new technological or organizational solutions.

Carrying out DPIAs enables us to identify the most effective way to comply with our data protection obligations and ensure the highest level of data privacy when processing. DPIA is part of our Privacy by Design approach and allows us to assess the impact and risk before carrying out the processing, thus identifying and correcting issues at the source, reducing costs, breaches and risks.

The DPIA enables us to identify possible privacy solutions and mitigating actions to address the risks and reduce the impact. Solutions and suggestions are set out in the DPIA and all risks are rated to assess their likelihood and impact. The aim of solutions and mitigating actions for all risks is to ensure that the risk is either: –

- Eliminated
- Reduced
- Accepted

7.0 Data Subject Rights Procedures

7.1Consent & The Right to be Informed

The collection of personal and sometimes special category data is a fundamental part of the products/services offered by the Company and we therefore have specific measures and controls in place to ensure that we comply with the conditions for consent under the data protection laws.

The data protection law defines consent as; *'Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a*

clear affirmative action, signifies agreement to the processing of personal data relating to him or her'.

Where processing is based on consent, the Company have reviewed and revised all consent mechanisms to ensure that: –

- Consent requests are transparent, using plain language and is void of any illegible terms, jargon or extensive legal terms
- It is freely given, specific and informed, as well as being an unambiguous indication of the individual's wishes
- Consent is always given by a statement or a clear affirmative action (*positive opt-in*) which signifies agreement to the processing of personal data
- Consent mechanisms are upfront, clear, granular (*in fine detail*) and easy to use and understand
- Pre-ticked, opt-in boxes are **never** used
- Where consent is given as part of other matters (i.*e. terms & conditions, agreements, contracts*), we ensure that the consent is separate from the other matters and is **not** be a precondition of any service (*unless necessary for that service)*
- Consent is always verifiable, and we have controls in place to ensure that we can demonstrate consent in every case
- We keep detailed records of consent and can evidence at a minimum: –
    - that the individual has consented to the use and processing of their personal data
    - that the individual has been advised of our Company name and any third party using the data
    - what the individual was told at the time of consent
    - how and when consent was obtained
- We have ensured that withdrawing consent is as easy, clear and straightforward as giving it and is available through multiple options, including: –
    - Opt-out links in mailings or electronic communications
    - Ability to opt-out in writing or by email
- For special category data, the consent obtained is explicit *(stated clearly and in detail, leaving no room for confusion or doubt*) with the processing purpose(s) always being specified

7.1.1 Consent Controls

The Company maintain records of data subject consent for processing personal data and are always able to demonstrate that the data subject has consented to processing of his or her personal data where applicable. We also ensure that the withdrawal of consent is as clear, simple and transparent and is documented in all instances.

Where the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent is presented in a manner which is clearly distinguishable from those matters, in an intelligible and easily accessible form, using clear and

plain language. All such written declarations should be reviewed and authorised by the Data Protection Officer prior to being circulated.

Consent to obtain and process personal data is obtained by the Company through: –

- In Writing
- Email
- Electronic *(i.e. via website form*)

Any electronic methods of gaining consent are regularly reviewed and tested to ensure that a compliant Privacy Notice is accessible and displayed and that consent is clear, granular and utilises a demonstrable opt-in mechanism.

Electronic consent is always by a non-ticked, opt-in action (*or double opt-in where applicable*), enabling the individual to provide consent after the below information has been provided.

Privacy Notices are used in all forms of consent and personal data collection, to ensure that we are compliant in disclosing the information required in the data protection laws in an easy to read and accessible format.

7.1.2 Information Provisions

Where personal data is obtained directly from the individual *(i.e. through consent, by employees, written materials and/or electronic formats (i.e. website forms, subscriptions, email etc*)), we provide the below information in all instances, in the form of a privacy notice: –

- The identity and the contact details of the Company
- The purpose(s) of the processing for which the personal information is intended
- The legal basis for the processing
- The recipients or categories of recipients of the personal data *(if applicable)*
- The existence of the right to request access to and rectification or erasure of, personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability
- The right to lodge a complaint with the Supervisory Authority
- The existence of any automated decision-making

The above information is provided to the data subject at the time the information is collected and records pertaining to the consent obtained are maintained and stored in line with the archival policy from the date of consent, unless there is a legal requirement to keep the information longer.

7.2 Privacy Notice

The Company defines a Privacy Notice as a document, form, webpage or pop-up that is provided to individuals at the time we collect their personal *data (or at the earliest possibility where that data is obtained indirectly)*.

Our Privacy Notice provides individuals with all the necessary and legal information about how, why and when we process their data, along with their rights and obligations.

We have a link to our Privacy Notice on our website and provide a copy of physical and digital formats upon request. The notice is accompanies our customer account opening forms which provides the legal information on how we handle, process and disclose personal information.

The notice is easily accessible, legible, jargon-free and is available in several formats, dependant on the method of data collection: –

- Via our website
- On account opening forms
- On agreements, contracts, forms and other materials where data is collected in writing
- In employee contracts and recruitment materials

7.3. Employee Personal Data

As per the data protection law guidelines, we do not use consent as a legal basis for obtaining or processing employee personal information. The contract of employment and HR policies ensure that employees are provided with the appropriate information disclosure and are aware of how the Company process their data and why.

All employees are provided with our Staff Handbook which informs them of their rights under the data protection laws and how to exercise these rights and are provided with a Privacy Notice specific to the personal information we collect and process about them.

7.4 The Right of Access

A data subject has the right to request access to personal data provided to the Company. Such information is provided free of charge and is in writing, or by other means where authorised by the data subject and with prior verification as to the subject's identity *(i.e. verbally, electronic*).

Information is provided to the data subject at the earliest convenience, but at a maximum of 30 days from the date the request is received. Where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further

months where necessary. However, this is only done in exceptional circumstances and the data subject is kept informed in writing throughout the retrieval process of any delays or reasons for delay.

Where we do not comply with a request for data provision, the data subject is informed within 30 days of the reason(s) for the refusal and of their right to lodge a complaint with the Supervisory Authority.

7.5 Data Portability

A data subject has the right to data portability. In exercising this right, the data subject has the right to have his or her personal data transmitted directly from one controller to another, where technically feasible. The Company provides all personal information pertaining to the data subject to them on request and in a format that is easy to disclose and read. We ensure that we comply with the data portability rights of individuals by ensuring that all personal data is readily available and is in a structured, commonly used and machine-readable format.

All requests for information to be provided to the data subject or a designated controller are done so free of charge and should be communicated within 30 days of the request being received. If for any reason, we do not act in responding to a request, we provide a full, written explanation within 30 days to the data subject or the reasons for refusal and of their right to complain to the supervisory authority.

All transmission requests under the portability right are assessed to ensure that no other data subject is concerned. Where the personal data relates to more individuals than the subject requesting the data/transmission to another controller, this is always without prejudice to the rights and freedoms of the other data subjects.

7.6 Rectification & Erasure

7.6.1 Correcting Inaccurate or Incomplete Data

Pursuant to Section 3.1 (7)(h) of the NDPR, data subject has the right to rectify his or her personal data. All data held and processed by the Company is reviewed and verified as being accurate wherever possible and is always kept up to date. Where inconsistencies are identified and/or where the data subject informs us that the data we hold is inaccurate, we take every reasonable step to ensure that such inaccuracies are corrected with immediate effect.

The relevant departments are notified of the data subjects request to update personal data and are responsible for validating the information and rectifying errors where they have been notified.

If for any reason, we are unable to act in response to a request for rectification and/or completion, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority.

7.6.2 The Right to Erasure

Also, known as *'The Right to be Forgotten'*, the Company shall comply fully with Section 3.1(9) where the Data Subject shall have the right to request the Controller to delete Personal Data without delay and the Company shall delete Personal Data where one of the following grounds applies:

- The Personal Data are no longer necessary in relation to the purposes for which they were collected or processed;
- The Data Subject withdraws consent on which the processing is based
- The Data Subject objects to the processing and there are no overriding legitimate grounds for the processing;
- The Personal Data have been unlawfully processed;
- The Personal Data must be erased for compliance with a legal obligation in Nigeria.

The right to be erased is not absolute and is only applicable in the scenarios listed in the regulation. If the Company previously made the personal data public or has disclosed it to others, the Company is required to take steps to inform all controllers processing the data of the data subject's request.

7.7 The Right to Restrict Processing

Article 3.1(13)**"**The Data Subject shall have the right to obtain from the Controller restriction of processing where one of the following applies:

- The accuracy of the Personal Data is contested by the Data Subject for a period enabling the Controller to verify the accuracy of the Personal Data;
- The processing is unlawful, and the Data Subject opposes the erasure of the Personal Data and requests the restriction of their use instead;
- The Controller no longer needs the Personal Data for the purposes of the processing, but they are required by the Data Subject for the establishment, exercise or defence of legal claims;
- The Data Subject has objected to processing, pending the verification whether the legitimate grounds of the Controller override those of the Data Subject.**"**

Any account and/or system related to the data subject of restricted data is updated to notify users of the restriction category and reason. When data is restricted, it is only stored and not processed in any way.

The right to restrict the processing of personal data is not absolute and is only applicable in the scenarios listed in the NDPR.

If the Data Controller previously made the personal data public or has disclosed it to others, they are required to take steps to inform all controllers processing the data of the data subject's request.

Data subjects who have requested restriction of data are informed within 30 days of the restriction application and are also advised of any third-party to whom the data has been disclosed. We should also provide in writing to the data subject, any decision to lift a restriction on processing. If for any reason, we are unable to act in response to a request for restriction, we should provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority.

7.8 Right to Objections

Data subjects are informed of their right to object to processing in our Privacy Notices and at the point of first communication, in a clear and legible form and separate from other information. We provide opt-out options on all direct marketing material and provide an online objection option where processing is carried out online. An objection may be in relation to all of the personal data that is held about an individual or only to certain information. It may also only relate to a particular purpose for processing the data.

The right to object is not absolute and is only applicable in the scenarios listed in the regulation. It is only applicable when the basis of processing is legitimate interest and public task.

Individuals have the right to object to: –

Where we are processing personal information for direct marketing purposes under a previously obtained consent, we will stop processing such personal data immediately where an objection is received from the data subject. This measure is absolute, free of charge and must always be adhered to.

7.9 Right around Automated Decision Making

Article 3.1(7L) Automated decision-making processes that do not involve human intervention. Prior to collecting Personal Data from a Data Subject, the Controller shall provide the Data Subject with all the following information:

- the existence of automated decision-making, including profiling and, at least, in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Data Subject;

We will also assess new systems and technologies for this same component prior to implementation. The Company understands that decisions absent of human interactions can be biased towards individuals and pursuant to Articles 3.1 (7L) of the data protection laws; we aim to put measures into place to safeguard individuals where appropriate.

In limited circumstances, the Company will use automated decision-making processes within the guidelines of the regulations. ***Such instances include: –***

- Where it is necessary for entering into or performance of a contract between us and the individual
- Where it is authorised by law *(e.g., fraud or tax evasion prevention)*
- When based on explicit consent to do so
- Where the decision does not have a legal or similarly significant effect on someone

Where the Company uses, automated decision-making processes, we always inform the individual and advise them of their rights. We also ensure that individuals can obtain human intervention, express their point of view and obtain an explanation of the decision and challenge it.

8.0 Oversight Procedures

8.1 Security & Breach Management

Alongside our *'Privacy by Design'* approach to protecting data, we ensure that all personal data held and processed by us is accounted for and recorded. Whilst every effort and measure are taken to reduce the risk of data breaches, the Company has procedures in place for notifications to be made to the Supervisory Authority and data subjects (where applicable).

9.0 Transfers & Data Sharing

The Company takes proportionate and effective measures to protect personal data held and processed by us at all times, however we recognise the high-risk nature of disclosing and transferring personal data and as such, place an even higher priority on the protection and security of data being transferred. In accordance with Article 2.12 of the NDPR, where a Data Controller or Data Administrator seeks to transfer Personal Data to a foreign country or an international organization, the NITDA shall examine if such country has adequate data protection law or regulation that can guarantee minimum privacy for the Personal Data of Nigerian citizens and residents. Where there is need for further legal cooperation from a target country, the NITDA may approach the office of Attorney-General for that purpose. In such circumstance, such data transfer and storage processes shall be done under the supervision of the Attorney-General. The Attorney General of the Federation may in its supervisory role prohibit the transfer of the Personal Data of Nigerian citizens or residents to certain countries where it is of the opinion that the country's data protection regime is inadequate or incompatible with Nigerian law.

Where data is being transferred for a legal and necessary purpose, compliant with all Articles in the Regulation, we ensure where possible data is subject to our data minimisation methods.

Conditions for Transfer of Personal Data to Foreign Countries

Any transfer of Personal Data which is undergoing processing or is intended for processing after transfer to a foreign country or to an international organization shall take place subject to the other provisions of the Regulation and the supervision of the Honorable Attorney General of the Federation (HAGF). The following are conditions for foreign transfer of personal data.

1. A transfer of Personal Data to a foreign country or an international organization may take place where the Agency has decided that the foreign country, territory or one or more specified sectors within that foreign country, or the international organization in question ensures an adequate level of protection

2. The HAGF shall take into consideration the legal system of the foreign country particularly in the areas of rule of law, respect for human rights and fundamental freedom, relevant legislation, both general and sectoral, including public security, Defence, national security and criminal law and the access of public authorities to Personal Data

3. Implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of Personal Data to another foreign country or international organization which are complied with in that country or international organization, case-law, as well as effective and enforceable Data Subject rights and effective administrative and judicial redress for the Data Subjects whose Personal Data are being transferred

4. The existence and effective functioning of one or more independent supervisory authorities in the foreign country or to which an international organization is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the Data Subjects in exercising their rights and for cooperation with the relevant authorities in Nigeria

5. The international commitments of the foreign country or international organization concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, particularly in relation to the protection of Personal Data.

Exceptions in Respect of Transfer to a Foreign Country

In the absence of any decision by The Agency or HAGF as to the adequacy of safeguards in a foreign country, a transfer or a set of transfers of Personal Data to a foreign country or an international organization shall take place only on one of the following conditions:

1. That the Data Subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers.

2. 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.

3. 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.

4. The transfer is necessary for important reasons of public interest

5. The transfer is necessary for the establishment, exercise or defense of legal claims

6. 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.

Countries With Adequate Data Protection Laws

S/N	COUNTRY						
1	All African - Countries who are signatories to the Malabo Convention 2014	12	Tunisia	23	Isle of Man	34	Qatar
2	All EU and European Economic Area Countries	13	Canada	24	Jersey	35	Singapore
3	Algeria	14	Cape Verde	25	Liechtenstein	36	South Korea
4	Argentina	15	China	26	Switzerland	37	Taiwan
5	Bahrain	16	Cyprus	27	Kenya	38	Turkey
6	Benin	17	Israel	28	United States of America	39	United Arab Emirates
7	Brazil	18	Japan	29	Guernsey	40	India
8	Ghana	19	Philippines	30	Japan	41	Uruguay
9	Mauritius	20	Singapore	31	Hong Kong		
10	South Africa	21	South Korea	32	Malaysia		
11	Togo	22	Faeroe Islands	33	Mauritius		

10.0 Audits & Monitoring

This shows the controls, measures and methods used by the Company to protect personal data, uphold the rights of data subjects, mitigate risks, minimise breaches and comply with the data protection laws and associated laws and codes of conduct. In addition to these, regular audits and compliance monitoring processes should be carried out with a view to ensuring that the

measures and controls in place to protect data subjects and their information, are adequate, effective, and compliant at all times.

The Data Protection Officer has overall responsibility for assessing, testing, reviewing and improving the processes, measures and controls in place and reporting improvement action plans to the Senior Management team where applicable. Data minimisation methods are frequently reviewed, and new technologies assessed to ensure that we are protecting data and individuals to the best of our ability.

All reviews, audits and ongoing monitoring processes should be recorded by the Data Protection Officer and will made readily available to the Supervisory Authority where requested.

The aim of internal data protection audits is to: –

- Ensure that the appropriate policies and procedures are in place
- To verify that those policies and procedures are being followed
- To test the adequacy and effectiveness of the measures and controls in place
- To detect breaches or potential breaches of compliance
- To identify risks and assess the mitigating actions in place to minimise such risks
- To recommend solutions and actions plans to Senior Management for improvements in protecting data subjects and safeguarding their personal data
- To monitor compliance with the data protection laws and demonstrate best practice

11.0 Training

Training will be provided to all employees on a general basis to ensure awareness of the requirements of the data protection laws and regulations. More focused training will be provided to Data protection champions. Training programme will also reflect new developments in the data protection laws. These training programs will be arranged for all staff members by Human Resources Department in conjunction with the Data Protection Officer. To this end, a regular training schedule/programme to cover all aspects of data protection law would be established and agreed annually between the DPO and HR unit.

This will ensure that all staff understand, have access to and can easily interpret the data protection laws requirements and its principles and that they have ongoing training, support and assessments to ensure and demonstrate their knowledge, competence and adequacy for the role. The training would include: –

- GDPR& NDPR Workshops & Training Sessions
- Scripts and Reminder Aids
- Access to GDPR & NDPR policies, procedures, checklists and supporting documents

Data privacy champions should be continually supported and trained in the data protection laws requirements.

12.0 Penalties

The Company understands its obligations and responsibilities under the data protection laws and recognises the severity of breaching any part of the law or Regulation. We respect the Supervisory Authority's authorisation under the legislation to impose and enforce fines and penalties on us where we fail to comply with the regulations, fail to mitigate the risks where possible and operate in a knowingly non-compliant manner.

We recognise that: –

- Breaches of the obligations of the controller, the processor, are subject to administrative fines up to
    a) in the case of a data controller dealing with more than 10,000 data subjects, to a fine of 2% of the Annual Gross Revenue of the preceding year or payment of the sum of N10 million, whichever is greater, and
    b) in the case of a data controller dealing with less than 10,000 data subjects, payment of a fine of 1% of the Annual Gross Revenue of the preceding year or payment of the sum of N2 million, whichever is greater
- Further, in the event that the data breach amounts to an offence under the Cybercrime Act, or any other sector-specific legislation, the person in breach may be subject to a term of imprisonment or additional fines or both, depending on the breach and the actions under the relevant law.