DATA PRORECTION & PRIVACY POLICY

Table of Contents

1.0.0 Introduction

As part of our operations, Pensions Alliance Limited ("PAL Pensions" or "the Company") collects and processes the personal information of individuals which could make such individuals easily identifiable. These individuals include past, current, and prospective employees, vendors, customers/clients and their representatives, next-of-kins and other individuals the Company communicates or deals with, jointly and/or severally ("Data Subjects").

Maintaining the Data Subject's trust and confidence requires that Data Subjects do not suffer consequences/effects as a result of providing the Company with their Personal Data. To this end, the Company is firmly committed to complying with applicable data protection laws, regulations, rules, and principles to ensure security of Personal Data handled by the Company. This Data Protection Policy ("Policy") describes the minimum standards that must be strictly adhered to regarding the collection, storage, use and disclosure of Personal Data and demonstrates the Company's dedication and commitment to processing Personal Data it receives or handles with absolute confidentiality and security.

This Policy applies to all forms of systems, operations and processes within the Company involving the collection, storage, use, transmission, and disposal of personal data.

Failure to comply with the data protection rules and guiding principles set out in the Nigeria Data Protection Regulations 2019 (NDPR) in addition to those set out in this Policy shall be considered a material violation of the Company's policies and may result in disciplinary action ..The Nigeria Data Protection Regulation (NDPR) is a piece of legislation that governs how the Company collects and processes personal data. Failure to comply with the NDPR may have severe consequences for the Company, including potential fines up to 2% of the Company's annual gross revenue from a preceding year or payment of the sum of N10,000,000 (ten million naira) whichever is greater, for the Company.

2.0.0 Scope

This Policy applies to all employees of the Company, external business partners (such as suppliers, contractors, vendors and other service providers) who receive, send, collect, access, or process Personal Data on behalf of the Company, including processing that is wholly or partly by automated means. The Policy also applies to third party data processors, who process personal data received from the Company

3.0.0 Purpose

The purpose of this Policy is outlined as follows:

- To protect the Company from the risks of a data breach.
- To disclose how the Company stores and processes personal data.
- To protect the rights of staff, members, and stakeholders of the Company.
- To comply with the NDPR, other applicable regulations and follow international best practices as relating to data protection.

4.0.0 Nigeria Data Protection Regulation

The Regulation, which came into force on January 25th 2019, regulates the gathering, storing and processing of personal data (regardless of whether data is stored electronically, on paper, or on other materials), and protects the rights and privacy of all living individuals (including children). The Regulation applies to natural persons residing in Nigeria or residing outside Nigeria but of Nigeria descent.

5.0.0 Applicability

Based on the provisions of the NDPR, the Company will be described as a data controller under the terms of the Regulation – this means the Company is ultimately responsible for controlling the use and processing of personal data. To ensure compliance, the Company shall appoint a Data Protection Officer (DPO) for the purpose of ensuring adherence to the NDPR, relevant data privacy statements and data protection directives of the Company.

The contact details of the Data Protection officer are as follows –

The Data Protection Officer
Pensions Alliance
289 Ajose Adeogun Street,
Victoria Island
Lagos, Nigeria
dataprotectionofficer@Palpensions.com

6.0.0 General Principles for Processing of Personal Data

The Company is committed to maintaining the principles in the NDPR regarding the processing of Personal Data. The following basic principles relating to the processing of personal data are adhered to demonstrate the commitment as well as the Company's aim of creating a positive privacy culture:

6.0.1 Lawfulness, Fairness and Transparency

Personal data must be processed lawfully, fairly and transparently at all times, as such, personal data collected and processed by or on behalf of the Company must be pursuant to a specific, legitimate and lawful purpose consented to by the Data Subject, save where the processing is otherwise allowed by law or within other legal grounds recognized in the NDPR.

6.0.2 Data Accuracy

Personal data must be accurate and kept up to date. In this regard, the Company shall make reasonable efforts to ensure the following:

a) Data collected and/or processed are accurate and not misleading in a manner that could be harmful to the Data Subject.

b) Reasonable and Applicable personal data are regularly updated

c) Timely correction of personal data on discovery of inaccuracies.

6.0.3 Purpose Limitation

The Company collects personal data for the purposes identified in the Company's privacy notice or other relevant document, based on any non–written communication (where applicable), provided to the Data Subject and for which consent is collected. Such personal data shall not be reused for purposes incompatible with those originally agreed, unless further consent is obtained.

6.0.4 Data Minimization

- The Company limits personal data collection and usage to data that is relevant, adequate, and necessary for carrying out the purpose for which such data is processed.
- The Company will evaluate the extent and need for processing personal data and where allowed, anonymized data must be used.

6.0.5 Integrity and Confidentiality

- The Company shall establish adequate controls to protect the integrity and confidentiality of personal data, both in digital and physical format and to prevent personal data from being accidentally or deliberately compromised.
- Personal data of Data Subjects must be protected from unauthorized access or viewing and from unauthorized changes to ensure its correctness.
- Any processing of personal data by an employee without a mandate to perform such will be considered

unauthorized and shall attract internal disciplinary actions.

- Employees may access personal data only as is appropriate for the type and scope of task in question and are forbidden to use such personal data for their own private or commercial purposes or to disclose or make such available to unauthorized persons.
- The Human Resources Department must inform employees at the start of the employment relationship of the obligation to maintain personal data privacy. This obligation shall remain in force even after an employees' employment ceases.

6.0.6 Accountability

- The Company shall show accountability consistent with the NDPR obligations by monitoring and continuously improving data privacy practices within the Company.
- Any individual or employee in breach of this Policy shall be subject to internal disciplinary action and could also face civil or criminal liability where their actions violate the law.

7.0.0 Data Privacy Policy

7.0.1 Overview

The Company considers personal data as confidential, and strives to adequately protect such data from unauthorized use and/or disclosure. The Company shall ensure that the Data Subjects are provided with adequate information regarding the use of their data as well as secure their requisite consent, where necessary. Also, the Company shall display a simple, visible and clear notice (Privacy policy) on any medium through which personal data is being collected or processed. The following information shall be considered for inclusion in the Privacy policy, as appropriate in distinct circumstances in order to ensure fair and transparent processing:

a) Data subjects' consent.
b) Description of collectable personal information.
c) Purpose of collection of personal data.
d) Technical methods used to collect and store personal information, cookies, web tokens, etc.
e) Access, if any, of third parties to personal data and purposes of such access.
f) A highlight of the principles governing data processing.
g) Available remedies in event of a violation of the privacy policy.
h) The timeframe for remedy.
i) Any limitation clause, provided that such limitation clause does not exonerate the operator from breaches of the Regulation

7.0.2: Pursuant to its statutory mandate of administering the pension savings of contributors and retirees under the Contributory Pension Scheme (CPS) in Nigeria, **Pensions Alliance Limited** (the PFA) collects and takes custody of the personal data of pension contributors, retirees and their related persons, such as beneficiaries and next-of-kins and their employers. The data include, but are not limited to, the biodata of contributors, retirees, and related persons.

This Data Privacy Policy (the Policy) is, therefore, instituted by the Company to inform pension contributors, retirees, and other related persons of the protection of their personal data collected and stored by the company's pursuant to the performance of its statutory responsibilities. The Policy also explains how the data are collected, stored and used. It highlights the few exceptional instances for disclosed.

7.1.0 Nature and reason for collection of personal data

7.1.1 Pursuant to the provisions of the Pension Reform Act (PRA) 2014 and extant regulations, the Company collects data of pension contributors, retirees, and their related persons. These may include name, gender, marital status, date of birth, nationality, National Identification Number, employment information and Next-of-Kin Information, amongst others.

Data collected and processed by Pensions Alliance may include but are not limited to:

a) Contact data (e.g. name, telephone, e-mail, address, IP address).
b) Key contract document data (Service Level Agreement, Non-Disclosure Agreement & product, or contractual interest).
c) Customer's account details
d) Employment history
e) Information about next of kin
f) Disclosed information (from third parties).
g) Employee and prospective employee data collected for recruitment and onboarding purpose.

Methods adopted by the company in the collection and storage of personal data may include but are not limited to:

a) Cookies.
b) CCTV recordings.
c) Physical and Online Forms
d) External hard drive
e) Audio and video call recordings

The Company collects the personal data of a pension contributor to open a Retirement Savings Account (RSA) and to administer the retirement benefits under the contributory pension scheme. In this regard, it is necessary, to collect some personal data of contributors to ensure that uniquely identifiable persons are registered under the CPS. It also facilitates the accurate computation of and remittance of pension contributions and other entitlements to the RSAs of contributors and the payment of benefits to them. Collection of data of the next-of-kin and beneficiaries of contributors, retirees and their related persons further ensures that the company has continuous access to the RSA holders.

7.2 Consent of Data Subject

Collection of data of the contributors, retirees and/or their related persons by the company shall be subject to the consent and authorization of the Data Subjects. Consequently, RSA registration and data recapture forms, including the electronic formats, contain data authorization clauses which are activated when the data subject completes the form.

7.3.1 Procuring Consent

Where the processing of Personal Data is based on consent, the Company shall obtain the requisite consent of the data subjects at the time of collection of Personal Data. In this regard, the company will ensure:

a) that Personal Data is not obtained except the specific purpose of collection is made known to the data subject
b) that the consent of Data Subject has been obtained without fraud, coercion, or undue influence
c) that the data subject has consented to processing of his or her personal data and has the legal capacity to give consent, where processing is based on consent
d) that request for consent is in a manner which is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language, where the data subject's consent is given in the context of a written declaration
e) that the Data Subject is informed of his/her right
f) that when assessing whether consent is freely given, the Company shall take account of whether the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is either not necessary or excessive for the performance of the contract
g) that the consent of the data subject is obtained where data may be transferred to a third party for any reason.

7.3.2 Valid Consent

For consent to be valid, it must be given voluntarily by an appropriately informed Data Subject. In

line with regulatory requirements, Consent cannot be implied. Silence, or inactivity does not constitute Consent under the NDPR.

7.3.3 Consent of Minors

The consent of minors (under the age of 18) will always be protected and obtained from minor's representatives following applicable regulatory requirements

7.4.0 Processing and Protection of Personal Data

The Company shall process the data of contributors, retirees and other related persons only for the purpose for which the data is collected. The Company shall process such data on both electronic and manual platforms, as may be required.

Only authorized officers of the Company shall have access to the personal data of pension contributors, retirees and related persons collected. Pursuant to Section 113 of the PRA 2014, such authorized persons shall include every member of the Board, officer, employee, agent or any other person engaged or authorized by the Company to examine any document or make an inquiry in relation thereto. Such authorized persons have a confidentiality obligation not to disclose or use any information or data of such person obtained directly or indirectly, except under the express authority of the Company or as otherwise provided for under this Policy.

7.5.0 Storage and Retention of Personal Data

7.5.1: The Company shall securely store the personal data of pension contributors, retirees and related persons that it collects in hard paper copies, computers, servers, and other electronic devices.

7.5.2: The Company shall hold Personal Data of contributor, retirees, and related persons for as long as may be deemed necessary to keep track of contribution remittances and payments of benefits. The retention period shall however not be less than 10 years, in line with the provisions of the National Archives Act, CAP.N6 Laws of the Federation of Nigeria, 2004.

7.6.0 Disclosure of Personal Data

7.6.1: Without prejudice to the foregoing provisions, however, the Company may be obliged to disclose personal data in its custody in the following circumstances:

- Where disclosure is made in compliance with statutory obligation or under an order of a court of competent jurisdiction.

- Where the Data Owner has expressly consented to the disclosure or instructed that his/her data be fully or partially disclosed to a named person; Provided that such consent or instruction may be withdrawn and communicated to the Company in writing at any time before disclosure.

Where the disclosure is made to the named person or organization for his/her personal use or record.

7.6.2 Transfer of Personal Data

- Third Party Data Processing Contracts
- To ensure compliance with the Regulation, being a Data Controller, the Company shall:
- Ensure that a written contract is signed by a third party that will process personal data of individuals
- Ensure that such third party that will process the data obtained from data subjects, complies with applicable laws and regulations

7.6.3 Transfer of Personal Data to Foreign Country

Where Personal Data is to be transferred to a country outside Nigeria, the Company shall put adequate measures in place to ensure the security of such Personal Data. In particular, the company shall, among other things, conduct a detailed assessment of whether the said country is on the National Information Technology Development Agency (NITDA) White List of Countries with adequate data protection laws.

The company shall comply with the Regulation and any transfer of personal data that is undergoing processing or is intended for processing after transfer to a foreign country or an international organization, shall take place subject to the provisions of the Regulation.

7.6.4 Exceptions in Respect of Transfer to a Foreign Country

In the absence of any decision made by NITDA or the Honorable Attorney General of the Federation (HAGF) on the transfer of personal data to a foreign country, the operator shall initiate the transfer or set of transfers of personal data to such foreign country or an international organization only when:

- The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers to the data subject due to the absence of an adequate decision and appropriate safeguards and that there are no alternatives.
- The transfer is necessary for the performance of a contract between the data subject and the Company or the implementation of pre-contractual measures taken at the data subject's request
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the operator and another natural or legal person
- The transfer is necessary for important reasons of public interest

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

The Company, in compliance with the Regulation, shall explicitly communicate through clear warnings, the specific principle(s) of data protection that is likely to be violated in the event of a transfer to a third country.

8.0.0 Violation of Data Privacy and Remedies

Contributors, retirees or their related persons whose data privacy rights are violated under this Policy shall report in writing, such violation to the Commission and The Company for immediate redress. Pursuant to the provisions of the PRA 2014 and extant Regulations of the Commission, the Commission shall direct The Company to redress the right of the affected contributor, retiree, or related person immediately. Failure of The Company to restore such rights as appropriate shall entitle the contributor, retiree or related person to legal remedies, subject to the provisions of the PRA 2014.

9.0.0 Governing Laws

This Data Privacy Policy is issued by the PFA, pursuant to the provisions of the PRA 2014, and is consistent with Sections 13 of the Constitution of the Federal Republic of Nigeria 1999 (as amended). It is also consistent with Clause 2.5 (a-i) of the Nigeria Data Protection Regulation 2019 issued by the National Information and Technology Development Agency (NITDA) and Article 8 of the International Convention on Data Protections.

10.0.0 Rights of Data Subjects

The Company shall:

- Take appropriate measures to provide any information relating to processing, to the data subject in a concise, transparent, intelligible, and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child
- Provide such information in writing, or by other means, including, where appropriate, by electronic means
- Provide any information relating to the processing of data obtained from the data subject orally, at the request of the data subject, provided that the identity of the data subject is proven by other means
- Inform the data subject without delay and at least within one (1) month of receipt of a request relating to the processing of his/her data, the reasons for not providing the information and the possibility of

lodging a complaint with the supervisory authority

- Provide information, any form of communication or any actions taken to a data subject free of charge
- Charge data subject if the request for his/her data is manifestly unfounded or excessive, in particular, because of his/her repetitive character. The charge shall be a reasonable fee considering the administrative costs of providing the information or communication or taking the action requested
- Write a letter to the data subject stating "refusal act" on the request and copy NITDA on every occasion through a dedicated channel which shall be provided for such purpose, provided that such request is excessive
- Bear the burden of demonstrating the manifestly unfounded or excessive character of the request
- Request for provision of additional information necessary to confirm the identity of the data subject where the operator has reasonable doubts concerning the identity of the requestor
- Provide the information in combination with standardized icons in order to give in an easily visible, intelligible, and legible manner, a meaningful overview of the intended processing and machine-readable format when presented electronically
- Provide the data subject with all of the following information, before collecting personal data:
    - The identity and the contact details of the pension operator
    - The contact details of the Data Protection Officer
    - The purposes of the processing for which the personal data are intended as well as the legal basis for the processing
    - The legitimate interests pursued by the operator or by a third party
    - The recipients or categories of recipients of the personal data, if any
    - Where applicable, the fact that the pension operator intends to transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by NITDA
    - The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
    - The existence of the right to request from each pension operator, 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 existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
    - The right to lodge a complaint with a relevant authority

- Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data
- 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
- Where the pension operator intends to further process the personal data for a purpose other than that for which collected, the operator shall provide the data subject prior to that further processing with information on that other purpose and with any relevant information
- Where applicable, that the pension operator intends to transfer personal data to a recipient in a foreign country or international organization and the existence or absence of an adequacy decision by NITDA

- Inform the data subject of the appropriate safeguards for data protection in the foreign country
- Rectify, without undue delay, inaccurate personal data concerning data subjects per their request
- Acknowledge the right of data subjects to have their incomplete data completed, including utilizing a supplementary statement
- 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 the 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 have to be erased for compliance with a legal obligation in Nigeria
- Take all reasonable steps to delete all the personal data made public and inform other companies processing the personal data of the data subject's request
- Acknowledge data subjects' rights to obtain restriction of processing their personal data where one of the following applies:
  - The accuracy of the personal data is contested by the data subject for a period enabling the operator 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 pension operator no longer needs the personal data for processing, but they are required by the data subject for the establishment, exercise, or defense of legal claims

- The data subject has objected to processing pending the verification to confirm whether the legitimate grounds of the operator override those of the data subject

- Process personal data with the data subject's consent, where processing has been restricted
- Communicate any rectification or erasure of personal data or restriction to each recipient to whom the personal data has been disclosed, unless this proves impossible or involves disproportionate effort
- Provide personal data concerning data subjects, in a structured manner, commonly used and machine-readable format to such data subjects
- Not hinder the data subject from transmitting those data in its database to another company where the processing is based on consent, on a contract and processing is carried out by automated means
- Execute data subjects' requests on the transmission of their data to another company, where technically feasible.at a reasonable cost.

Data Subjects can exercise any of their rights by completing the company's Subject Access Request (SAR) Form and submitting to the Company via

dataprotectionofficer@palpensions.com

11.0.0 Data Breach Management Procedure

A data breach procedure is established and maintained in order to deal with incidents concerning Personal Data or privacy practices leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

All employees must inform their designated line manager or the Data Processing Officer of the company immediately about cases of violations of this Policy or other regulations on the protection of Personal Data, following the company's Personal Data Breach Management Procedure in respect of any:

a) improper transmission of Personal Data across borders.
b) loss or theft of data or equipment on which data is stored.
c) accidental sharing of data with someone who does not have a right to know this information.
d) inappropriate access controls allowing unauthorized use.
e) equipment failure.
f) human error resulting in data being shared with someone who does not have a right to know; and
g) hacking attacks.

11.0.1 Notification

A data protection breach notification must be made immediately after any data breach occurs. This is to ensure that the supervisory authority shall at least:

- 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.

- communicate the name and contact details of the data protection officer or other contact point where more information can be obtained.
- describe the likely consequences of the personal data breach.
- describe the measures taken or proposed to address the personal data breach, including measures to mitigate its possible adverse effects.

In case there is a significant chance of adverse effects on the data subject, the data subject is also duly notified about the breach. The information given includes that:

a) the controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it.
b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize.

.

11.0.2 Potential Breach

When a potential breach has occurred, the company will investigate to determine if an actual breach has occurred and the actions required to manage and investigate the breach as follows:

a) Validate the Personal Data breach.
b) Ensure proper and impartial investigation (including digital forensics if necessary) is initiated, conducted, documented, and concluded.
c) Identify remediation requirements and track resolution.
d) Report findings to the top management.
e) Coordinate with appropriate authorities as needed.
f) Coordinate internal and external communications; and
g) Ensure that impacted Data Subjects are properly notified, if necessary.

Reporting of data breach to a Data Protection Authority is very important under the NDPR. Data breaches are to be reported within 72 hours after becoming aware of it

.12.0.0 Data Protection Impact Assessment

As part of the risk and audit assessment, the Company shall carry out a Data Protection Impact Assessment (DPIA) in respect of any new project or IT system involving the processing of Personal Data to determine whenever a type of processing is likely to result in any risk to the rights and liberties of the Data Subject.

13.0.0 Data Security

All Personal Data must be kept securely and should not be stored any longer than necessary. The Company will ensure that appropriate measures are employed against unauthorized access, accidental loss, damage, and destruction to data. This includes the use of password, encryption of databases for digital storage and locked cabinets for those using a paper form.

To ensure the security of Personal Data, the Company will, among other things, implement the following appropriate technical controls:

a) Develop security measures including but not limited to protecting systems from hackers
b) Set up firewalls and protect email systems
c) Store data securely with limited access to specifically authorized individuals
d) Employ data encryption technologies on workstation/laptops. Also implementing encryption at rest including key management
e) Develop an organizational policy for handling personal data and other sensitive or confidential data
f) Continuously build capacity for all staff
g) Industry-accepted hardening standards i.e. enhancing the system's security features which include (the use of strong passwords for authentication, minimizing unnecessary software etc.), for workstations, servers, and databases.
h) Enable Security Audit Logging across all systems managing Personal Data.
i) Restrict the use of removable media such as USB flash, disk drives.
j) Anonymization techniques on testing environments; and
k) Physical access control where Personal Data is stored in hardcopy.

.14.0.0 Personnel Training

The Company shall ensure that employees who collect, access and process Personal Data receive adequate data privacy and protection training in order to develop the necessary knowledge, skills and competence required to effectively manage the compliance framework under this Policy and the NDPR concerning the protection of

Personal Data. On an annual basis, the Company shall develop a capacity building plan for its employees on data privacy and protection in line with the NDPR.

15.0.0 Data Protection Audit Assessment

The Company shall conduct periodic data protection audits through a licensed Data Protection Compliance Organization (DPCOs) to verify the company's compliance with the provisions of the NDPR and other applicable data protection laws.

The audit report will be certified and filed by the DPCO to NITDA as required under the NDPR.

16.0.0 Definitions

- **"NDPR**" means the Nigerian Data Protection Regulation, 2019.

- **"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; It can be anything from a name, address, a photo, an email address, bank details, PIN number, 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 (PII) and others.

- **"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.
- **"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"** means characters, symbols and binary, on which operations are performed by a computer which may be stored or transmitted in the form of electronic signals stored in any format or any device
- **"Database"** means a collection of data organized in a manner that allows access, retrieval, deletion and procession of that data; it includes but not limited to structured, unstructured, cached and file system type databases

- **"Data Administrator"** means a persons or organization that processes data
- **"Data Controller"** means a person who either alone, jointly with other persons or in common with other persons or as a statutory body, determines the purposes for and how personal data is processed or is to be processed
- **"Data Portability"** means the ability for data to be transferred easily from one IT system or computer to another through a safe and secure means in a standard format
- **"Nigeria Information Technology Development Agency"** - NITDA
- **"Data Protection Compliance Organization"** (DPCO) means any entity duly licensed by NITDA for training, auditing, consulting and rendering services and products for compliance with this Regulation or any foreign Data Protection law or regulation having effect in Nigeria
- **"Data Subject"** means an identifiable person; one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity
- **"Party"** means directors, shareholders, servants, and privies of a contracting party
- **"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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
- **"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 transmitted, stored, or otherwise processed
- **"Record"** means public record and reports in a credible news media
-
- **"Regulation"** A rule or instruction made and maintained by an authority

16.0.1 Roles and Responsibilities

In compliance with the Regulation, below are some stakeholders and their responsibilities to drive the operationalization of the Policy and implementation of necessary data protection controls within the company.

Board

- Set the tone at the top on data protection
- Ultimately responsible for ensuring that the Company meets the obligations of the Regulation

Executive Management Committee

- Ensure data protection objectives are established and are aligned with the strategic direction of the Company
- Ensure that the resources needed for the protection of data are available
- Communicate the importance of effective data protection in the Company and of conforming to its requirements
- Support other relevant Management roles to demonstrate their leadership as it applies to their areas of responsibility

Head, Branding and Communication

- Approve in conjunction with legal any data protection statements attached to communications such as emails and letters
- Approve in conjunction with legal, responses to any data protection queries from journalist or media outlets such as newspaper
- Provide directives that ensures marketing initiatives abide by data protection principles

Data Protection Officer

- Keep Executive Management updated about data protection responsibilities, risks, and issues
- Review all data protection procedures and related policies, in line with an agreed schedule
- Arrange data protection training and advice for the people covered by the Policy
- Handle data protection questions from staff and anyone else covered by the Policy
- Deal with requests from individuals to obtain the data PenOp holds about them
- Review and approve any contracts or agreements with third parties that may handle the Company's sensitive data

Head, Information Communication Technology

- Ensure all systems, services and equipment used for storing data meet acceptable security standards
- Evaluate any third-party services the pension operator is considering using to store or process data such as private cloud computing services

Information Security Unit

- Perform regular checks and vulnerability scans to ensure adequate security of hardware and software used in data processing

Head, Internal Audit Department

- Provide reasonable assurance regarding the achievement of the operational objectives, such as the effectiveness and efficiency of the security controls
- Carry out internal audit and report findings to Executive Management
- Recommend preventive and corrective action

17.0 Review and Enquiries

This Privacy Policy is subject to review by the Company from time to time as the need arises. All enquiries regarding the Policy should be directed to:

The Managing Director
289 Ajose Adeogun Street
Victoria Island
Lagos.

18.0 Consequences

The consequence of not adhering to the Policy will be handled in line with the Company's Disciplinary Policy.

19.0 Appendix

Related Policies and Procedures

This Policy shall be read in conjunction with the following policies and procedures of the company:

- IT Security Policy.
- Data governance policy
- Archiving Policy.
- Privacy Notices & Cookies Policy
- Pre-employment Privacy Notice

20.0 Reference(s)

- Nigeria Data Protection Regulation, 2019
- Data Protection Policy