PRUDENTIAL ZENITH LIFE INSURANCE

DATA PROTECTION POLICY

Document version number	1.0
Document Status	Proposed
Document Date	April 2019

APPROVAL

NAME	**DATE**
Enterprise Risk Management and Governance Committee	May 2019
PZL Board	May 2019

VERSION CONTROL

Version	Date	Description
1.0	April 2019	Document Creation

Date of next policy review: May 2020

Contents

Definitions 4
Introduction 5
Policy objectives 5
Scope 5
Framework and Governance 5
Applicable Laws and Regulations 7
Lawful Processing 7
Privacy Notices 7
Communications to Data Subjects 7
Purpose Limitation 7
Data Minimisation 8
Data Accuracy 8
Storage Limitation 8
Data Security 8
Breach Handling and Reporting 8
Data Transfers 9
Data Subject Rights 9
Third Party Processors 9
Privacy Risk Assessments 9
Product and Process Development 10
Records and Registers 10
Registration Requirements 10
Training 10
Policy Review 10
Appendix A: PZL Data Classification 10

Definitions

Applicable Data Protection Laws: All national, international and local laws, regulations and rules by any government, agency or authority relating to data protection and privacy which are applicable to Prudential Zenith Life Insurance "PZL".

Data Controller: A person who either alone, jointly with other persons or in common with other persons or a statutory body determines the purposes for and the manner in which Personal Data is processed or is to be processed in line with the PZL requirements.

Data Processing: Any operation or set of operations which is performed on 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.

Data Subject: Any persons whose personal data would be collected, held and processed by PZL.

Personal Data: Any information relating to an identified or identifiable natural person. It can be anything from a name, address, telephone number, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier such as an online identifier. This includes any expression of opinion about a living individual or any indication PZL's intentions about the individual.

Personal Data Breach: 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

Introduction

This Data Protection Policy (the "Policy") document is part of a set of Group risk policies that address the risks to which Prudential Zenith Life Insurance Limited "PZL" is exposed. It is a local adaption of the Group Privacy Policy. PZL is an organization which considers data protection as a key driver for a sustainable business. The policy outlines how PZL manages compliance with the Nigeria Data Protection Regulation 2019 through the definition and distribution responsibilities within and outside the organization.

PZL will take all reasonable steps to ensure that Personal Data is processed fairly and in accordance with applicable data protection laws. The Company is committed to implementing appropriate organisational and technical measures to achieve this aim

PZL collects data of individual and corporate customers to deliver life insurance services. This policy defines guidelines on how this data is to be processed.

Policy objectives

The objective of the Policy is to set the framework by which the Company can ensure a level of data protection commensurate with its regulatory and legal obligations, while meeting the demands of a global competitive and commercial organisation.

Scope

This Policy forms part of the Group Governance Manual ("GGM"). Certification of compliance with this Policy is included in the certifications required by the GGM. This policy applies to all personal data PZL collects, holds and/or processes regardless of the location where such data may be stored which may be on an employee's device, a partner organization, contractor or agent performing work on behalf of or in conjunction with PZL. A failure to comply with this policy may result in disciplinary action in accordance with PZL's current disciplinary procedures.

Framework and Governance

It is the responsibility of executive management to ensure full compliance with all local regulatory and statutory requirements of the Nigeria Data Protection Regulation and the Group Privacy Policy. Areas where these requirements are perceived to be in conflict must be communicated to the Group Data Privacy Lead.

Governance of the policy rests with the Chief Risk and Compliance Officer.

Individuals are responsible for considering the privacy implications of any tasks and activities that they may be asked to undertake, ensuring where necessary, that they escalate concerns to management.

PZL shall:
GPP3 - Work closely with the Group Privacy Office through the Regional Risk Officer to ensure that the requirements of this Policy have been implemented.

GPP 4 – Fulfill the roles and responsibilities as defined below (and any others that may be assigned by the Group):

1. PZL Board and Management
   The PZL Board of directors is ultimately responsible for defining the purposes for and the manner in which Personal Data is processed or is to be processed. The Board may delegate to Executive Management as it deems fit.

2. Executive Management
   The Executive Management 'ExCo' will act as an advisory body to the PZL Board of Directors on matters relating to the collection, processing and security of data. The ExCo will also be charged with the responsibility of providing oversight on the implementation of this policy as requested by the MD/CEO.

3. Data Protection Officer
   The Data Protection Officer shall be appointed by the ExCo and the officer shall be responsible for;

- Developing, maintaining and administering the data protection policy.
- Monitoring compliance with the provisions of this policy.
- Assisting other employees in understanding the data protection process.

4. All Employees
   All PZL Employees shall:

- Ensure strict adherence to this policy.
- Ensure they are familiar with the requirements of the Data Protection Act, and other regulatory requirements as they relate to data protection.
- Disclose information to others on a need to know basis only. The need for access must be demonstrated at all times. (The PZL Data Classification guidelines is referenced in appendix 1)
- Inform the Data Protection Officer of any new requirement, products, or processes that relates to data processing.
- Ensure appropriate documentations are in place prior to any data sharing arrangements with a 3rd party
- Ensure that all data is processed securely by complying with PZL's information security, access control and password policies
- Ensure only information that they are authorized to access is processed
- Report data protection breaches and vulnerabilities in a timely manner to the Information Technology Team and the Data Protection Officer

GPP 5 – Cooperate with the Group Privacy Office to assess and report on compliance with this Policy and privacy risks in accordance with the Privacy Accountability Framework (described in the data protection and privacy Group-wide Operating Standards "GwOS").

Applicable Laws and Regulations

GPP 6 – It is PZL's policy to comply fully with the Nigeria Data Protection Regulation 2019 and all regulatory requirements to which the Company is required to adhere to. This applies to retrieval, storage, processing, retention and disposal of personal data.

Lawful Processing

GPP 7 – PZL shall only process Personal Data of its employees for due diligence and record keeping purposes. PZL shall process its customers' data for policy inception, risk management, assurance review purposes and where a lawful ground to do so has been established.

Privacy Notices

GPP 8 – PZL shall provide Data Subjects with clear and easily accessible statements about the Processing of their Personal Data.
At a minimum such statements shall include:

- the identity and the contact details of the Data Controller;
- the contact details of the Data Protection Officer;
- the categories of Personal Data being collected;
- the purpose and intended scope for which the Personal Data is collected;
- any disclosures of Personal Data to third parties**.**

GPP 9 – Subject to the Nigeria Data Protection Regulation 2019, GPP 8 shall not apply where:

- the Data Subject already has the information;
- the provision of such information proves impossible or would involve disproportionate effort; or
- obtaining or disclosure of personal data is expressly laid down by applicable laws and this permits obtaining or disclosure without providing the information in GPP 8.

Communications to Data Subjects

GPP 10 - When communicating with Data Subjects about their Personal Data, PZL shall provide information in a concise, transparent, intelligible and easily accessible form using clear and plain language.

GPP 11 - Communications by PZL to Data Subjects shall take place within reasonable timeframes and without undue delay.

Purpose Limitation

GPP12 – PZL shall ensure that all Personal Data is collected for specified, explicit and legitimate purposes only as stated above and not further processed in a manner that is incompatible with those purposes.

GPP 13 – In the event that Personal Data is to be used for a purpose other than that for which it was

originally collected, PZL shall:

- reassess the lawful ground for processing the Personal Data; and
- establish that the Personal Data can be processed in accordance with a lawful ground
- seek the consent of the data subject to administer the data for the new purpose.

Data Minimisation

GPP14 – PZL shall ensure Personal Data collected is adequate, relevant and limited to what is necessary for the purposes for which they are processed.

Data Accuracy

GPP15- PZL shall ensure Personal Data are accurate and, where necessary, kept up to date.

Storage Limitation

GPP16- PZL shall ensure Personal Data is kept for no longer than is necessary for the purposes for which the data is processed, unless other legal requirements applies. Data shall be stored archived in line with PZL's records retention policy.

Data Security

GPP17- PZL shall adopt applicable security measures detailed in the Group Security Policy, the Group Privacy Policy and this Policy.

GPP18- PZL shall ensure data is secured by implementing deliberate risk based measures as stated in the Group Security and Privacy policy, e.tc.

Breach Handling and Reporting

GPP19- PZL shall ensure that all Personal Data Breaches are handled in accordance with the requirements of the Group Security Policy, the Group Privacy Policy and this Policy.

GPP20- In the event of a material personal data breach, PZL shall collate the following information:

- 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;
- an assessment of the likely consequences of the personal data breach to PZL and impacted Data Subjects;
- the measures taken or proposed to be taken by PZL to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Data Transfers

GPP21- PZL shall ensure that personal data is not transferred across Nigeria's borders unless**:**

- the use of the personal data is in accordance with the purposes communicated to the Data Subject; or
- the Data Subject has consented to the transfer; or
- the transfer is otherwise permissible in accordance with applicable data protection laws.

GPP22- PZL shall remain accountable for personal data under its control regardless of its location.

GPP23- PZL shall document personal data transferred across Nigeria's borders including electronic access by individuals or entities in another country. This documentation must as a minimum include:

- the recipient identity,
- the Personal Data source,
- the Personal Data transferred
- purpose of the transfer,
- method of transfer,
- security measures taken to protect the Personal Data.

Data Subject Rights

GPP24- PZL shall comply with Data Subject rights to the extent specified in applicable Data Protection Laws.

Third Party Processors

GPP25- PZL shall ensure that all Processing of Personal Data by a third party is in accordance with the requirements of the Group outsourcing, Third party supply policy privacy and this policy.

GPP26- Where processing is to be carried out on behalf of PZL, PZL shall use only data processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of applicable Data Protection Laws.

GPP27- PZL shall ensure that processing carried out by a third party Data Processor is governed by a contract or other legal act under applicable laws, that is binding on the Data Processor. The Data Processor shall process personal data in accordance with the PZL's instructions and shall implement appropriate technical and organisational measures to protect Personal Data at all times

Privacy Risk Assessments

GPP28- PZL shall conduct a privacy risk assessment when undertaking new processing activities involving Personal Data or where there are significant changes to an existing Processing activity.

Product and Process Development

GPP29- When introducing new technology, systems, applications and/ or processes, PZL shall implement appropriate technical and organisational measures to achieve compliance with applicable data protection laws.

Records and Registers

GPP30- PZL maintains a record of data processing activities. This is broadly described below-

Data Subjects	Processing Activities	Personal Data
Individuals Corporate entities	Underwriting and Reinsurance Risk Assessment Claims Settlement Assurance Review	Names Revenue/Annual Emolument Contact Information Occupation Health status

Coinsurers, reinsurers, professional advisers, local and international regulatory bodies, and/or other third parties as may be required by law are the recipients to whom the Personal Data may be or will be disclosed and or transferred to. All recipients of the data shall be managed in line with the third party processor provisions of this policy.

Security measures have been defined in GPP17 and GPP18

Registration Requirements

GPP31- PZL shall satisfy all registration requirements with the appropriate data protection authority

Training

GPP32- PZL shall ensure all employees, contractors and any other individuals who Process Personal Data for or on behalf of the PZL are trained on the data protection policies which shall be communicated to them.

They will be required to attest that they understand the provisions of the policy as well as their role and responsibilities in the implementation of the policy.

Policy Review

This policy is subject to review and change annually or as regulatory and business requirements demand.

Appendix A: PZL Data Classification

Data Class	Description	Examples
DC1	Data acceptable for public use without restrictions.	• Promotion Flyers • Product Flyers • Information available on the Corporate Website
DC2	Data sensitive in nature with restrictions on distribution within and outside PZL and or the Group	• Financial and Technical Data • Employee Data
DC3	Data more sensitive in nature not expected to be distributed outside PZL or the Group and restricted to the Board, ExCo and any other party as the Board deems fit	• Strategy Road Maps • Any data meant to give PZL competitive advantage