PremiumTrust Bank

Data Protection Policy

Classification: Internal
April 2023
Document Number: PTB/ICS/23/0008
Status: Approved

Document Control Sheet

Version and Update History

Date	Document Version	Document Revision History	Document Author/Reviser
March 2023	1.0	Document creation	Information & Cyber Security Group

Change Control

Change Clause/Frequency
The contents of this document are subject to change control on a twelve (12) months review cycle.

Contents

Tables

1 Introduction

PremiumTrust Bank Limited, as a data controller and processor, is committed to conducting its business in accordance with the Nigeria Data Protection Regulation (NDPR) and global best practices concerning the protection of personal data and safeguard of individuals privacy to ensure compliance with the Data Protection requirements.

In its daily business operations, PremiumTrust Bank makes use of a variety of data about identifiable individuals, including data about:

- Employees
- Customers
- Website users
- Other stakeholders

In collecting and using these personal data, the Bank is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it.

The purpose of this policy is to set out the relevant legislation and to describe the steps that the Bank is taking to ensure that it complies with it. The policy is also to ensure that PremiumTrust Bank processes personal data in a way that is consistent with all data protection and privacy guidelines, to protect the "rights and freedoms" of individuals, and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

This control applies to all systems, people and processes that constitute the Bank's information systems, including board members, directors, employees, suppliers and other third parties who have access to PremiumTrust Bank systems.

The following policies and procedures are relevant to this document:

- Data Protection Impact Assessment Process
- Personal Data Analysis Procedure
- Information Security Incident Response Procedure
- NDPR Roles and Responsibilities
- Records Retention and Protection Policy

Non-compliance may expose PremiumTrust Bank to complaints, regulatory actions, fines or/and reputational damage.

2 Data protection policy

- **The Nigeria Data Protection Regulation**

The Nigeria Data Protection Regulation (NDPR) is one of the most significant pieces of legislation affecting the way that PremiumTrust Bank carries out its information processing activities. Significant fines are applicable if a breach is deemed to have occurred under the NDPR, which is designed to protect the personal data of Nigerian citizens. It is PremiumTrust's policy to ensure that compliance with the NDPR and other relevant legislation is always clear and demonstrable.

- **Data Protection Objectives**

The objectives of the data protection framework are that it should enable the Bank to:

- meet its own requirements for the management of personal data,
- meet the requirements of the Nigeria Data Protection Regulation (NDPR), and
- protect the interests of natural persons and other key stakeholders.

- **Definitions**

There are a total of 27 definitions listed within the NDPR and it is not appropriate to reproduce them all here. However, the most fundamental definitions with respect to this policy are as follows:

- **Personal data:**

Defined as "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**

"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."

- **Controller**

"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.

- **Processor**

The natural or legal person or an organization that processes personal data on behalf of the data controller.

- **Special Categories of Personal Data**

Are 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.

- **Data Subject**

Any living individual who is the subject of personal data held by an organisation.

- **Personal Data Breach**

A breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

- **Consent**

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.

- **Third party**

A natural or legal person, public authority, agency, or body other than the data subject, controller, processor, and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

Principles relating to processing of personal data

There are several fundamental principles upon which the NDPR is based. These are as set out in Part Two: 2.1 of the NDPR as follows:

❖ **Paragraph 1**

Personal data shall be:

a) *Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');*
b) *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 the NDPR, not be considered to be incompatible with the initial purposes ('purpose limitation');*
c) *Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');*
d) *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');*
e) *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 the NDPR subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');*
f) *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').*

❖ **Paragraph 2**

The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

❖ **Compliance with principles relating to personal data**

PremiumTrust Bank will ensure that it complies with all these principles both in the processing it currently carries out and as part of the introduction of new methods of processing such as new IT systems.

- **Rights of the individual**

The data subject also has rights under the NDPR. These consist of:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Each of these rights is supported by appropriate procedures within PremiumTrust Bank that allow the required action to be taken within the timescales stated in the NDPR. These timescales are shown in Table 1.

DATA SUBJECT REQUEST	TIMESCALE
The right to be informed	When data is collected (if supplied by data subject) or within one month (if not supplied by data subject)
The right of access	One month
The right to rectification	One month
The right to erasure	Without undue delay
The right to restrict processing	Without undue delay
The right to data portability	One month
The right to object	On receipt of objection

Rights in relation to automated decision making and profiling.	Not specified

Table 1: Timescales for data subject requests

- **Lawfulness of processing**

  There are six alternative ways in which the lawfulness of a specific case of processing of personal data may be established under the NDPR. It is PremiumTrust Bank policy to identify the appropriate basis for processing and to document it, in accordance with the Regulation. The options are described in brief in the following sections.

  - **Consent**

    Unless it is necessary for a reason allowable in the NDPR, PremiumTrust Bank will always obtain explicit consent from a data subject to collect and process their data.

    In case of children below the age of 18, parental consent will be obtained. Although, the Bank does not offer services directly to children.

    Transparent information about our usage of their personal data will be provided to data subjects at the time that consent is obtained and their rights regarding their data explained, such as the right to withdraw consent. This information will be provided in an accessible form, written in clear language and free of charge.

    If the personal data are not obtained directly from the data subject, then this information will be provided to the data subject within a reasonable period after the data are obtained and within one month (30 days).

  - **Performance of a contract**

    Where the personal data collected and processed are required to fulfil a contract with the data subject, explicit consent is not required. This will often be the case where the contract cannot be completed without the personal data in question.

  - **Legal obligation**

    If the personal data is required to be collected and processed to comply with the law or regulatory requirement, then explicit consent is not required. This may be the case for some data related to employment, KYC obligations, or taxation.

- **Vital interests of the data subject**

  In a case where the personal data are required to protect the vital interests of the data subject or of another natural person, then this may be used as the lawful basis of the processing. PremiumTrust Bank will retain reasonable, documented evidence that this is the case, whenever this reason is used as the lawful basis of the processing of personal data. As an example, this may be used in aspects of social care, or when processing is critical to save a person's life.

- **Task carried out in the public interest**

  Where PremiumTrust Bank needs to perform a task that it believes is in the public interest or as part of an official duty, then the data subject's consent will not be requested. The assessment of the public interest or official duty will be documented and made available as evidence, where required.

- **Legitimate interests**

  If the processing of specific personal data is in the legitimate interests of PremiumTrust Bank and is judged not to affect the rights and freedoms of the data subject in a significant way, then this may be defined as the lawful reason for the processing. Again, the reasoning behind this view will be documented.

- **Data protection by design**

  PremiumTrust Bank has adopted the principle of data protection by design and will ensure that the definition and planning of all new or significantly changed systems that collect, or process personal data will be subject to due consideration of data protection issues, including the completion of one or more data protection impact assessments (DPIAs).

  The data protection impact assessment will include:

  - Consideration of how personal data will be processed and for what purposes.
  - Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s).
  - Assessment of the risks to individuals in processing the personal data.
  - What controls are necessary to address the identified risks and demonstrate compliance with the regulation.

  Use of techniques such as data minimization, encryption, anonymisation, and pseudonymisation will be considered where applicable and appropriate.

- **Contracts involving the processing of personal data**

  PremiumTrust Bank will ensure that all relationships it enters that involve the processing of personal data are subject to a documented contract that includes the specific information, clauses, and terms required by the NDPR.

- **International transfers of personal data**

  Transfers of personal data outside Nigeria will be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the NDPR. This depends partly on the Honourable Attorney General of the Federation (HAGF)'s judgement as to the adequacy of the safeguards for personal data applicable in the receiving country and this may change over time.

  Intra-group international data transfers will be subject to legally binding agreements referred to as Binding Corporate Rules (BCR) which provide enforceable rights for data subjects.

- **Data Protection Officer**

  A defined role of Data Protection Officer (DPO) is required under the NDPR if an organisation is a public authority, if it performs large scale monitoring or if it processes particularly sensitive types of data on a large scale. The DPO is required to have an appropriate level of knowledge and can either be an in-house resource or outsourced to an appropriate service provider.

  Based on these criteria, PremiumTrust Bank requires a Data Protection Officer to be appointed. The Data Protection Officer, who the Management Board considers to be suitably qualified and experienced, has been appointed to take the responsibility for PremiumTrust's compliance with this policy daily. The DPO has direct responsibility for ensuring that the Bank complies with the NDPR, as do Management/Executive Directors in respect of data processing that takes place within their area of responsibility.

  PremiumTrust's Data Protection Officer is responsible for reviewing and updating essential data protection compliance documentations annually, in the light of any changes to Bank's operations and activities, and to any additional requirements identified by means of data protection impact assessments. A register of changes needs to be available on the supervisory authority's request and in the event of an audit.

- **Roles & Responsibilities**

The DPO has specific responsibilities in respect of procedures such as the Subject Access Request Procedure and is the first point of call for Employees/Staff seeking clarification on any aspect of data protection compliance.

Compliance with the NDPR is also the responsibility of all PremiumTrust's employees/staff who use/process personal data. The Bank's Training plan sets out specific training and awareness requirements in relation to specific roles and employees of PremiumTrust generally.

Roles	Responsibilities
Management Board	• Driving compliance with the NDPR in line with the policy provisions • Encourage the adoption of good information handling practices within PremiumTrust Bank.
Data Protection Officer	• Develop, review, and evaluates this policy document. • Accountable to the Bank's Management board for the management of personal data within PremiumTrust Bank. • Ensures that compliance with data protection legislation and good practice can be demonstrated. • Accountable for development and implementation of the data protection requirements, as required by this policy. • Accountable for security and risk management in relation to compliance with this policy
Chief Information Security Officer/Head of IT	• Responsible for convening meetings of the Management board, either after there have been (or it is planned that there will be) significant changes in the organisational environment, business circumstances, legal conditions, or technical environment, and which is likely to have an impact on the level of risk facing personal data, or at least annually

- **Breach Notification**

  Under the NDPR, the Nigeria Data Protection Bureau (NDPB) has the authority to impose a range of fines of up to two percent of annual worldwide turnover or ten million naira, whichever is the higher, for infringements of the regulation.

  It is PremiumTrust Bank's policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. In line with the NDPR, where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed within 72 hours. This will be managed in accordance with the Bank's Information Security Policy Manual, which sets out the overall process of handling information security incidents.

- **Addressing Compliance to the NDPR**

  The following actions are undertaken to ensure that PremiumTrust Bank always complies with the accountability principle of the NDPR:

  - The legal basis for processing personal data is clear and unambiguous.
  - A Data Protection Officer is appointed with specific responsibility for data protection within the Bank.
  - All staff involved in handling personal data understand their responsibilities for following good data protection practice.
  - Training in data protection to be provided to all staff members.
  - Rules regarding consent are followed.
  - Routes are available to data subjects wishing to exercise their rights regarding personal data and such enquiries are handled effectively.
  - Regular reviews of procedures involving personal data are carried out.
  - Privacy by design is adopted for all new or changed systems and processes.
  - The following documentation of processing activities is recorded:
    - Organisation name and relevant details
    - Purposes of the personal data processing
    - Categories of individuals and personal data processed.
    - Categories of personal data recipients
    - Agreements and mechanisms for transfers of personal data to foreign countries including details of controls in place.
    - Personal data retention schedules
    - Relevant technical and organisational controls in place

  These actions are reviewed on a regular basis as part of the management process concerned with data protection.

- **Data Protection Policy Review**

  PremiumTrust Bank maintains a culture of continuous monitoring, review, and improvement with regards to compliance with the data protection standard and to identify possible areas of non-compliance before they escalate into a risk, which might affect mitigation actions where necessary.

  All relevant, essential documents, including data collection forms will be reviewed annually to ensure they effectively reflect the regulatory provisions.

  Before making any inputs or approving the policy document, Management will examine the review status from previous document version, relevant NDPR changes (if any), and any other relevant data protection performance information.

  The output of the Management review process will include, but not limited to:

  - Modifying or improving policies and procedures and their effectiveness, ensuring that any changes to business operations or processes, or changes to statutory, regulatory, or contractual requirements are accommodated.
  - Improving the allocation of resources and responsibilities, including ensuring that complying with the regulation enjoys adequate Management support via adequate resources, funding, and budget.
  - Formulating and approving any changes to the Data Protection Policy that would be necessary to give effect to any improvements identified.

  The Management board must approve any changes to the policy at its next scheduled meeting and prior to its implementation.