PremiumTrust Bank

Data Retention Policy

Classification: Internal
April 2023
Document Number: PTB/ICS/23/0014
Status: Approved

Document Control Sheet

Version and Update History

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

Change Control

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

Table of Contents

1. Introduction

1.1 PremiumTrust Bank Limited as an organization holds a great deal of information that is crucial to the running of its daily business operations. While many information systems can be recovered after an incident, the business-critical data that resides in electronic and hard copy forms must be suitably protected. This involves considerations as to the Confidentiality, Integrity, and Availability (CIA) of business critical and potentially sensitive data.

1.2 PremiumTrust Bank must comply with our obligations under data protection laws (including the Nigeria Data Protection Regulation ["NDPR"] and the General Data Protection Regulation ["GDPR"]) whenever we process personal data or sensitive data relating to our employees, workers, customers and suppliers and any other individuals we interact with.

1.3 This includes the obligation not to process any personal data which permits the identification of data subjects for longer than is necessary and the purpose of this policy is to assist us to comply with that obligation. This policy should be read alongside the Data Retention Schedule which is appended at Appendix to this policy, and which provides guideline on data retention periods for the various types of personal data or sensitive data we hold.

1.4 Compliance with this policy will also assist us to comply with our 'data minimisation' and accuracy obligations under data protection laws which require us to ensure that we do not retain personal data, which is irrelevant, excessive, inaccurate, or out of date.

1.5 A failure to comply with data protection laws could result in enforcement action against the Bank, which may include substantial fines of up to 10 million Naira or 2% of total worldwide annual turnover (whichever is higher), significant reputational damage and potential legal claims from individuals.

1.6 Compliance with this policy will also assist in reducing the Bank's information storage costs and the burden of responding to requests made by data subjects under data protection laws such as access and erasure requests.

1.7 We are also required under data protection laws to inform data subjects about how long we will retain their personal data in our privacy notices.

1.8 This policy is for internal-use only and cannot be shared with third parties, customers, or regulators without prior authorisation from our Data Protection Officer.

1.9 For definitions of terms used in this policy, please refer to the Definitions appended at Section 2 to this policy (Appendix).

2. Purpose

The purpose of this data retention policy is to provide guidance on the retention of the various types of data PremiumTrust Bank holds. This document strives to balance the need to store information so that it can be accessed for as long as it is needed with legal obligations to destroy the data safely when it is no longer required.
Appropriate and effective protection is required for all types of data that PremiumTrust Bank holds. This is to promote business continuity and avoid breaches of statutory, regulatory and/or contractual obligations.

3. Scope

All PremiumTrust Bank's records, whether analogue or digital, are subject to the retention requirements of this policy. This data retention policy applies to information in all its various forms. It may be on paper, stored electronically or held on film, or other media. It includes text, pictures, audio, and video. It covers information transmitted by post, by electronic means, and by oral communication, including telephone and voicemail. It applies throughout the lifecycle of the information from creation through storage and utilization to disposal.

4. Policy

4.1 The Bank is required under data protection laws to ensure that Information Assets containing Personal Data are not retained for any longer than is necessary for the purposes for which the Personal Data have been collected. We must be able to justify our retention of Personal Data to the authority responsible for enforcing data protection laws in Nigeria, Nigeria Data Protection Bureau.

4.2 In practice, what this means is that the Bank must not retain the Personal Data contained within Information Assets for any longer than is necessary:

a) For the operational purpose that the Personal Data was collected for, and which the relevant Data Subject has been informed of (i.e., in relevant privacy notices);
b) To comply with any applicable statutory or regulatory retention requirements; or
c) To enable the Bank to exercise its legal rights and/or defend against legal claims.

4.3 Where a statutory or regulatory retention requirement applies, or where data is relevant to an actual or potential legal claim, only the specific Personal Data which is required to be retained in order to meet the

statutory/regulatory retention requirement or for a legal claim, should be retained for those purposes.

4.4 We must take a proportionate approach to data retention, balancing our needs with the impact of retention on Data Subjects' privacy. We also need to comply with all other aspects of data protection laws in relation to the Personal Data we retain, including, but not limited to, ensuring that its retention is fair and lawful and that it is secured by appropriate technical and organizational measures against unauthorized or unlawful processing, and against accidental loss, destruction, or damage.

4.5 Guideline for data retention periods for different types of Personal Data, which should be followed by all employees, are provided in the Data Retention Schedule in Appendix.

4.6 We must ensure that any request received from a Data Subject asking us to delete or destroy their Personal Data under the 'right to be forgotten' is dealt with in accordance with data protection laws.

4.7 Each Information Asset owner must ensure that effective processes are in place to ensure that the Personal Data within their control is retained, archived, and deleted or destroyed in accordance with this policy and the Data Retention Schedule.

4.8 Prior to the expiry of the retention period for the Personal Data provided in the data Retention schedule (or at regular intervals, and at least annually if no such retention period is provided), the Personal Data should be reviewed by the Information Asset owner to determine whether the Bank should continue to retain it (or any part of it), for operational reasons, in order to comply with a statutory retention period or a regulatory obligation or for the purposes of a legal claim.

4.9 If Personal Data needs to be retained only for statutory or regulatory purposes or for a legal claim, the Information Asset owner should ensure that it is moved from a live environment to a secure archive that is subject to appropriate security and restricted access to ensure that the Personal Data is only used for that specified purpose. Once it is no longer needed for that purpose, it is the responsibility of the Information Asset owner to ensure that the Personal Data is securely and permanently deleted or destroyed or anonymised in accordance with paragraph 5 of this policy.

4.10 Any queries about the applicable retention period for Personal Data within

an Information Asset (for example, if there is no applicable data retention period in the Data Retention Matrix for that data) should be directed to the Data Protection Officer.

5. Secure Deletion or Anonymising Data

5.1 Where there is no need to retain Personal Data any longer, it is the responsibility of the Information Asset owner to ensure that the Personal Data is securely and permanently deleted or destroyed in accordance with this policy or that it is anonymised. Personal Data is anonymised where no Data Subjects can be identified from the data, either from that data alone or together with other data that the Bank holds, has access to or may obtain access to. This also applies to any back-ups or duplicate copies of the Personal Data.

5.2 Personal Data must be deleted or destroyed using one of the following secure methods:

a) Documents retained electronically should be deleted with a secure deletion utility that ensures that the information cannot be retrieved. Standard deletion utilities that only remove the file pointer should not be used.
b) Personal Data on hard drives, removable media and any similar items must be securely erased before any disposal or reassignment of the equipment. Accepted methods include utilities that meet the ISO 270001 standard or by encrypting the entire contents of the medium to at least AES-256 and irretrievably deleting the encryption key.
c) Where Personal Data cannot be erased from equipment, it must be physically destroyed by an authorised specialist destruction company, and certificates of destruction must be obtained.
d) Paper copies must be destroyed using cross-cut shredders.

5.3 The Information Asset owner must approve the destruction or deletion of the Personal Data in advance and must record it including the date (and time if relevant), the content of the Personal Data and the method of destruction or deletion. They must also liaise with the Data Protection Officer to ensure that our Records of Processing Activities are amended accordingly. Once Management approval is in place, representatives from Information and Cyber Security Group, Compliance, Internal Audit, and Corporate Services will join the team to witness the disposal process.

6. Responsibility

6.1 Information Asset owners are/responsible for ensuring that all Personal Data is collected, retained, and destroyed in line with the requirements of the NDPR.

The following roles are responsible for retention of these records because they are the Information Asset Owners:

a) The **Chief Financial Officer (CFO)** is responsible for retention of financial (accounting, tax) and related records.
b) The **Chief People Officer (CPO)** is responsible for retention of all personnel/employee records.
c) The **Chief Legal Counsel/Company Secretary** is responsible for retention of all other statutory and regulatory records.
d) The **Chief Compliance Officer (CCO)** is responsible for monitoring compliance.
e) The **Head, Operational Risk Management** is responsible for ensuring that retained records are included in business continuity and disaster recovery plans.
f) The **Data Protection Officer** is responsible for storage of data in line with this procedure.

6.2 Compliance with this policy is overseen by the Data Protection Officer and Chief Compliance Officer. The Data Protection Officer will retain a record of the training provided to personnel to ensure that they understand the Bank's data retention and destruction obligations, their own responsibilities, and the internal processes they need to follow.

6.3 Information Asset owners are responsible for ensuring that all Information Assets containing Personal Data that are within their control are retained and destroyed in accordance with this policy and the Data Retention Schedule. They must implement measures to ensure that they can identify when a retention period is due to expire, so that they can carry out a review and determine whether the Personal Data should be deleted or destroyed. In addition, Information Asset owners should carry out periodic reviews at least annually of the Personal Data contained in the Information Assets that are within their control (even if that Personal Data is not covered by a retention period contained in the Data Retention Matrix), to determine whether it is being retained and destroyed in accordance with this policy. Information Asset owners may delegate routine tasks, where appropriate.

6.4 This policy applies to all Bank personnel ("you" or "your") and it sets out what we expect from you to assist the Bank to comply with its data retention and destruction obligations under data protection laws. All Bank personnel play a vital role, and you must read and ensure that you fully understand and comply with this policy in relation to all Personal Data which you process on our behalf, and you must attend all related training provided.

6.5 Your compliance with this policy is mandatory. Any breach of this policy may result in disciplinary action.

7. Review and Disposal

Before any records are destroyed, they should be reviewed to ensure records that need to be retained beyond the scheduled retention date are not destroyed and that an appropriate method of disposal is selected.

A record should be kept of documents approved for disposal. An appropriate method of disposal should be selected bearing in mind the sensitivity of the records including, whether they are personal or sensitive data.
Ordinary refuse disposal (trash bin) should only be used for non-sensitive records, while personal or sensitive data should be securely erased or deleted. Documents containing Personal Data or Sensitive data shall be disposed of in the following ways:

- Shredding – hard copy documents
- Secure deletion – soft copy documents

Care shall be taken to ensure documents are not stolen, copied, leaked to unauthorized personnel during the process of destruction/deletion.

Appendix

1. Guideline Retention Periods

1.1. PremiumTrust Bank is legally required to keep certain corporate data for defined periods of time.

1.2. A retention period of 6 years is recommended for any record or document in active use period unless an exception has been obtained granting a shorter or longer active use period by the business unit or department responsible for creating, using, processing, disclosing, storing, and destroying the record.

1.3. For the purposes of enforcing retention in accordance with this Data Retention policy, each department should be responsible for the records and documents it creates, uses, stores, processes and destroys.

1.4. All PremiumTrust Bank employees should be responsible for preserving, maintaining, and managing records in their possession in accordance with this policy and any additional customer- imposed obligations.

1.5. PremiumTrust Bank must request business partners involved in the records management, such as physical records storage and technology outsourcing, to conform to PremiumTrust Bank data management policies, standards, and processes.

1.6. All PremiumTrust Bank employees should be responsible for managing all PremiumTrust Bank records that are in their individual possession, custody, and/or control. This includes organizing such records so that only related items with common subject matter and retention periods are assembled for storage purposes (e.g., in the same file folder, CD, or box).

1.7. Personal Data and business records should be stored in an appropriate manner to ensure record integrity and to enable records tracking for easy access and retrieval.

1.8. Examples of corporate information not subject to the retention policy include:

a) Document copies kept for personal convenience or reference (unless it contains Personal Data, where the document may be created in full compliance with applicable privacy laws and retained no longer than stated in the retention schedule as it applies to the original document).

b) Publications, trade journals, and magazine articles that require no action. Routine correspondence (unless relevant to a customer or other business transaction).

c) Inter-office notices (including email) such as meeting requests and internal announcements.

d) Cryptographic keys.

1.9. PremiumTrust Bank employees need to make electronic copies of all paper records, where applicable, using the same naming convention and filing system for reference purposes.

1.10. All paper records and electronic data need to have basic metadata attributes or labels to identify data that would be pertinent for the retrieval or destruction of such records, including record category, record date(s), record owner, customer name, anticipated destruction date, and a description of the contents.

1.11. PremiumTrust Bank employees should exercise caution if they are uncertain whether a particular data category is subject to a defined retention period. When in doubt, preserve the data and consult the designated Data Protection Officer.

1.12. The least retention period for the various data record categories is summarized as follows:

Guideline Retention Periods

Type of Record	**Retention Period**
Recruitment records - These may include: Completed online application forms or CVs. Equal opportunities monitoring forms. Assessment exercises or tests. Notes from interviews and short-listing exercises. Pre-employment verification of details provided by the successful candidate. For example, checking qualifications and taking up references. Criminal records check.	For unsuccessful candidates 6 - 12 months after notifying candidates of the outcome of the recruitment exercise. These records may be transferred to a successful candidate's personnel file if they are relevant to the ongoing employment relationship.
Employee Records	**Active** – For the duration of the employee's employment **Archive** – 6 years after the employee's employment ends.
Customer Data	**Active** – For the duration of the customer's contract with the bank. **Archive** – 6years following termination of an account or business relationship.
Audit Logs	**Active** – 6 months **Archive** – 2 years
Accounting and Financial Records	**Active** – 3 years **Archive** – 6 years

Marketing Records	**Active** – 2 years **Archive** – 3 years
Procurement and Contract records	**Active** – For the life of the contract **Archive** – 4 years
Legal Records	**Active** – For the duration of the case. **Archive** – '6 years but may be kept indefinitely for future use subject to the Chief Legal Counsel justifying the necessity for retaining any of the records
Other Records	**Active** – 5 years **Archive** – 1 year or in accordance with local laws and regulations.

2. **Definition of Terms**

Controller	A controller determines the purposes and the means of the processing of personal data. It has the power to make high-level decisions about how and why the personal data can be used. It determines matters such as, the content of the data to be collected and used, who it will be collected about and when it will be disclosed and to whom.
Data Subjects	The individuals to whom the Personal Data relates, such as employees or job applicants, customers, or suppliers.
Information Assets	A piece or body of information (regardless of the form it takes, i.e., paper, electronic records or correspondence, photographs, CD/DVDs, CCTV etc.) such as an employee record, a customer list, or a financial report that is processed by or on behalf of the Bank.
Personal Data	Any information relating to an identified or identifiable individual. An identifiable individual is one who can be identified either directly from data, or indirectly, either on its own or

	together with other data, which is in, or may come into, the Controller or Processor's possession. For example, by reference to a name, identification number, location data, IP address, online identifier or to other factors such as physical or economic factors.
Process or Processing	Any operation or set of operations carried out in relation to personal data, such as collecting, storing, disclosing, amending, and deleting. Processing is widely defined and will in effect cover any activity involving personal data, for example, storing CVs, updating employee, customer, or supplier records, monitoring employees' internet use, or operating a CCTV system which captures Data Subjects' behaviour, etc.
Processor	A processor merely processes the personal data on behalf of the Controller. It is not able to make high-level decisions about how and why the data will be used.
Special Categories of Personal Data	Personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life/sexual orientation, genetic data, or biometric data for the purpose of uniquely identifying a natural person.
Supervisory Authority	The regulatory authority responsible for enforcing data protection laws in Nigeria.