Data Protection and Privacy Policy

Document Number: UBN/DOC/NDPA/060

Document Classification: Internal

Release Date: January 2026

Table of Contents

1.0 Introduction

As part of our operations, Union Bank of Nigeria Plc (hereinafter referred to as "Union Bank" or "The Bank") collects and processes certain types of Personal Data that can be used to identify an individual. These include, but are not limited to:

- **General Personal Data:** name, surname, e-mail address, city, phone, Identification numbers, nationality, BVN, next of kin details, occupation, marital status, guarantor details, Date of Birth (DOB) etc.

- **Sensitive Data:** passport photograph, signature, medical records **(for staff and job applicants)**
- **Financial Data:** account numbers, transaction history, payment instructions, loan/credit information, credit history etc.
- **Device & Technical Data:** IP address, device ID, geolocation data, digital channel usage logs.
- **Biometric Data (where applicable):** fingerprints, facial recognition, or other authentication-related biometrics.
- **Behavioural Data:** Page visits, link clicks, content engagement metrics, Communication channel preferences, consent status etc.
- **Customer Interaction Data:** call recordings, chat transcripts, complaint submissions.
- **Security & Access Data:** CCTV footage, visitor logs, access control records.

These categories apply to current, past and prospective employees, merchants, suppliers/vendors, customers, partners, and any other individuals whom Union Bank interacts with ("Data Subjects").

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

This Policy applies to all forms of systems, operations and processes within Union bank environment that involve 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 Act, 2023 (NDPA), General Application and Implementation Directive, 2025 (GAID) as well as those set out in this Policy is a material violation of Union bank's policies and may result in disciplinary action as required, including suspension or termination of employment or business relationship.

1.1 Data Privacy Commitment and Mission

UBN is committed to monitoring and continually improving the protection of data to meet our privacy responsibilities to our customers, staff, vendors and regulators, and to reduce expenses to legal sanction, operational loss or reputational damage. We are committed to ensuring:

- The confidentiality of personal data in our keep
- The integrity and availability of such personal data
- The compliance to regulatory and legal requirements are met
- That data privacy and security training is provided to staff
- Notify the Commission of personal data breaches within seventy-two (72) hours of becoming aware of the breach.
- The maintenance of our ISO 27001 certification.
- Notify a data subject immediately after becoming aware of a personal data breach that may pose high risk to his or her privacy

2. Scope

This Policy applies to all employees of Union bank, as well as to any external business partners (such as merchants, suppliers, contractors, vendors and other service providers) who receive, send, collect, access, or process Personal Data in any way on behalf of Union bank, including processing wholly or partly by automated means. This Policy also applies to third party Data Processors who process Personal Data received from Union bank.

3. General Principles for Processing of Personal Data

Union bank is committed to maintaining the principles in the NDPA/GAID regarding the processing of Personal Data.

To demonstrate this commitment as well as our aim of creating a positive privacy culture within Union bank, Union Bank adheres to the following basic principles relating to the processing of Personal Data:

3.1 Lawfulness, Fairness and Transparency

Personal Data must be processed lawfully, fairly and in a transparent manner at all times. This implies that Personal Data collected and processed by or on behalf of Union bank must be in accordance with the 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 NDPA and GAID

3.2 Data Accuracy

Personal Data must be accurate and kept up-to-date. In this regard, Union bank:

a) shall ensure that any data it collects and/or processes is accurate and not misleading in a way that could be harmful to the Data Subject;

b) make efforts to keep Personal Data updated where reasonable and applicable; and

c) make timely efforts to correct or erase Personal Data when inaccuracies are discovered.

3.3 Purpose Limitation

Union bank collects Personal Data only for the purposes identified in the appropriate Union Bank Privacy Notice provided to the Data Subject and for which Consent has been obtained. Such Personal Data cannot be reused for another purpose that is incompatible with the original purpose, except a new Consent is obtained.

The purposes for which Union bank will use your personal data includes:

a) **For the provision of services to you**. For example, when you purchase any of our products, we will use your personal data to process your order.

b) **For customer care and billing**. When you use our products, we will use your personal information to bill you and to respond to enquiries and concerns that you may have about our products and services.

c) **Customer service messages.** We will use your personal data to keep you updated with the latest information or changes about our products and services.

d) **For marketing purposes**. In order to serve you better, will use your personal data to market our products and services to you.

3.4 Data Minimization

Union bank limits Personal Data collection and usage to data that is relevant, adequate, and absolutely necessary for carrying out the purpose for which the data is processed.

Union bank will evaluate whether and to what extent the processing of personal data is necessary and where the purpose allows, anonymized data must be used.

3.5 Integrity and Confidentiality

Union bank shall establish adequate controls in order 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 viewing or access and from unauthorized changes to ensure that it is reliable and correct.

Any personal data processing undertaken by an employee who has not been authorized to carry such out as part of their legitimate duties is un-authorized.

Employees may have access to Personal Data only as is appropriate for the type and scope of the task in question and are forbidden to use Personal Data for their own private or commercial purposes or to disclose them to unauthorized persons, or to make them available in any other way.

Human Resources Department must inform employees at the start of the employment relationship about the obligation to maintain personal data privacy. This obligation shall remain in force even after employment has ended.

3.6 Personal Data Retention

All personal information shall be retained, stored and destroyed by Union bank in line with legislative and regulatory guidelines. For all Personal Data and records obtained, used and stored within Union bank, Union bank shall perform periodical reviews of the data retained to confirm the accuracy, purpose, validity and requirement to retain.

To the extent permitted by applicable laws and without prejudice to Union bank's Document Retention Policy, the length of storage of Personal Data shall, amongst other things, be determined by:

(a) the contract terms agreed between Union bank and the Data Subject or as long as it is needed for the purpose for which it was obtained; or

(b) whether the transaction or relationship has statutory implication or a required retention period; or

(c) whether there is an express request for deletion of Personal Data by the Data Subject, provided that such request will only be treated where the Data Subject is not under any investigation which may require Union bank to retain such Personal Data or there is no

subsisting contractual arrangement with the Data Subject that would require the processing of the Personal Data; or

(d) whether Union bank has another lawful basis for retaining that information beyond the period for which it is necessary to serve the original purpose.

Notwithstanding the foregoing and pursuant to the NDPA/GAID, Union bank shall be entitled to retain and process Personal Data for archiving, scientific research, historical research or statistical purposes for public interest.

Union bank would forthwith delete Personal Data in Union bank's possession where such Personal Data is no longer required by Union bank or in line with Union bank's Retention Policy, provided no law or regulation being in force requires Union bank to retain such Personal Data.

3.7 Accountability

Union bank demonstrates accountability in line with the NDPA/GAID obligations by monitoring and continuously improving data privacy practices within Union bank.

Any individual or employee who breaches this Policy may be subject to internal disciplinary action (up to and including termination of their employment); and may also face civil or criminal liability if their action violates the law.

4. Data classification & handling requirements

Union Bank shall classify all information assets to ensure appropriate levels of protection are applied. Personal Data shall be classified according to its sensitivity and risk impact level.

The following classification tiers shall apply:

1. Public Data: Information intended for public disclosure with minimal risk if exposed.
2. Internal Data: Non-public business information whose unauthorized disclosure may cause operational inconvenience.
3. Confidential Data (Personal Data): Information that identifies or can identify a Data Subject. Unauthorized disclosure may cause harm, financial loss, or reputational damage.
4. Restricted/Highly Confidential Data: Sensitive Personal information whose exposure poses severe risk, including health data, biometrics, political opinions, religious beliefs, or children's data, financial plans, strategic plans etc.

All Personal and Sensitive Personal Data must be safeguarded in accordance with their classification level.

4.1 Handling Requirements

- Personal Data must not be transferred via unsecured channels.
- Sensitive Personal Data must be encrypted during transmission and storage.
- Access to Personal Data must follow strict need-to-know principles.
- Printed Personal Data must be stored in locked cabinets and destroyed via secure shredding.

5. Data Privacy Notice

5.1 Union Bank considers Personal Data as confidential and as such must be adequately protected from unauthorized use and/or disclosure. Union bank will ensure that the Data Subjects are provided with adequate information regarding the use of their Personal Data as well as acquire their respective Consent, where necessary.

5.2 Union Bank shall display a simple and conspicuous notice (Privacy Notice) on any medium through which Personal Data is being collected or processed. The following information must be considered for inclusion in the Privacy Notice, as appropriate in distinct circumstances in order to ensure fair and transparent processing:

a) Description of collectible Personal Data.
b) Purposes for which Personal Data is collected, used and disclosed.
c) What constitutes Data Subject's Consent.
d) Purpose for the collection of Personal Data.
e) The technical methods used to collect and store the information;
f) Available remedies in the event of violation of the Policy and the timeframe for remedy; and
g) Adequate information in order to initiate the process of exercising their privacy rights, such as access to, rectification and deletion of Personal Data.

5.3 Union bank Privacy Notice is available on Bank's website via this link https://www.unionbankng.com/privacy-policy

5.4 Union Bank shall maintain and routinely update an enterprise-wide Data Inventory that documents all systems, applications, databases, and business processes that collect or process Personal Data.

5.5 Union bank shall maintain a ROPA containing the following details for each processing activity:

- Category of Personal Data processed
- Purpose of processing
- Categories of Data Subjects
- Lawful Basis for processing
- Recipients of Personal Data
- Retention period

- Cross-border transfer requirements
- Security safeguards applied
- Relevant data owner or system custodian

The ROPA shall be reviewed annually and maintained by the Data Protection Officer (DPO).

5.6 Union Bank maintains a Data Governance structure to ensure oversight of Personal Data management across the enterprise. The structure includes:

- Data Protection Officer (DPO): Provides oversight, guidance, and compliance monitoring.
- Data Owners: Departmental heads responsible for ensuring Personal Data processed within their units complies with this Policy.
- Data Stewards: Operational personnel responsible for implementing privacy controls within their processes.
- Information Security Team: Ensures appropriate technical and organizational security measures.
- Internal Audit / Compliance: Independently reviews adherence to privacy obligations.

This structure ensures clear accountability and distributed responsibility for data privacy across Union bank.

5.7 Union bank shall adopt the principles of Privacy by Design and Default for all new products, systems, services, and processes that involve Personal Data. This includes:

- Embedding privacy controls at the early stages of system and process design.
- Limiting Personal Data collection to what is strictly necessary (data minimization).
- Ensuring default settings do not expose Personal Data unnecessarily.
- Ensuring ongoing review of system updates, changes, and third-party integrations.

All new technology initiatives must undergo a review by the DPO and Information Security prior to implementation.

5.8 Where Union bank uses cookies or tracking technologies on its digital platforms:

- Strictly Necessary Cookies shall be enabled by default.
- All other cookies (Performance, Functional, Analytics) require explicit consent.
- Data subjects may withdraw cookie consent at any time through the cookie management interface.
- Cookie identifiers and tracking data shall be treated as Personal Data where applicable under the NDPA.

6. Legal Grounds For Processing Of Personal Data

5.1. The personal data we collect from our customers and how we collect it depends on the services that our customers subscribe to, how they use our services and how they interact or interface with us. This also applies to persons who are not customers of Union bank but have interacted with Union bank. We may also obtain your personal data from a third party with permission to share it with us.

Please note that we only process your personal data based on the grounds set out in the NDPA/GAID. Accordingly, in line with the provisions of the NDPA/GAID, processing of Personal Data by Union bank shall be lawful if at least one of the following applies:

a) where you give us consent to the processing of your Personal Data for one or more specific purposes. You are at liberty to withdraw the consent and Union bank will cease to process your personal where there is no other basis to do so.

b) where the processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;

c) processing is necessary for compliance with a legal obligation to which Union bank is subject;

d) processing is necessary in order to protect the vital interests of the Data Subject or of another natural person;

e) processing is necessary for the performance of a task carried out in the public interest or in exercise of official public mandate vested in Union bank; and

f) processing is necessary for the purpose of the legitimate interest pursued by the data controller or data processor, or by a third party to whom the data is disclosed.

Interests in personal data processing shall not be legitimate for the purposes of Paragraph 5.1.
(f), where;

a) They override the fundamental rights, freedoms and the interests of the data subjects;
b) They are incompatible with other lawful basis of processing listed in Paragraph 5.1.1 above; and
c) The data subject would not have a reasonable expectation that the personal data would be processed in the manner envisaged.

The table below sets out the major types of personal data, the purposes for which they are processed, and the applicable lawful bases.

S/N	PURPOSE OF COLLECTION	TYPE OF DATA	LAWFUL BASIS

1	Regulatory Actions	Name, Phone Number, Email Address, Contact Address, Sex, Date of Birth, Photograph.	Legal Obligation. Some instances may involve public interest.
2	Employment	Name, Phone, Email Address, Contact Address, Sex, Date of Birth, Photograph, Medical Record, Educational Record.	Contract. Some instances may involve other bases such as consent, vital interest, or legal obligation.
3	Account Opening & Customer Onboarding	Name, BVN, NIN, Address, Phone Number, Email Address, Identification Documents (passport, driver's license), Photograph, Signature, Occupation.	Contract, legal obligation and consent for non-essential, optional processing.
4	Know-Your-Customer (KYC) & Anti-Money Laundering (AML) Checks	Identification Data, Biometric Data (where applicable), Financial History, Transaction Patterns, Address Verification Data.	Legal Obligation.
5	Provision of Banking & Financial Services	Account Information, Transaction Data, Contact Details, Device Information (for digital channels), Payment Instructions.	Contract: necessary to perform the service requested by the Data Subject.
6	Loan & Credit Processing	Employment Data, Financial Records, Credit History, Guarantor Information, Identification Details.	Contract, Legal Obligation, (creditworthiness assessment).
7	Fraud Monitoring & Security Operations	Transaction Monitoring Data, Device Data, IP Address, Location Data, Transaction Anomalies.	Legal Obligation, Public Interest,

8	Customer Service & Complaint Resolution	Contact Details, Account Details, Call Recordings, Complaint Submissions.	Contract
9	Digital Banking Access & Authentication	Username, Password, Device ID, IP Address, Geolocation, Biometrics (where applicable).	Contract and Consent (for biometrics).
10	Marketing & Customer Engagement	Contact Information, Demographic Data, Product Usage, Preferences.	Consent; Data Subject may withdraw at any time.
11	Vendor & Third-Party Management	Business Contact Details, Identification Data of Vendor Representatives, Compliance Documents.	Contract, Legal Obligation.
12	Risk Management & Reporting	Transaction Records, Financial Data, Behavioral Data, Internal Monitoring Reports.	Legal Obligation, some instances may involve public interest.
13	Legal Claims, Investigations & Enforcement	Identification Data, Transaction Data, Communication Records.	Legal Obligation, Public Interest
14	Business Continuity & Disaster Recovery	Backup Records, Contact Information, System Logs.	Legal Obligation
15	Access Control & Physical Security	CCTV Footage, Visitor Logs, Biometric Access Data (where applicable).	Legal Obligation, and Consent (for biometrics).
16	Training & Quality Assurance	Call Recordings, Chat Transcripts, Performance Metrics.	Contract (for employees).
17	Stakeholder Communication & Notifications	Contact Details, Account Details, Service Subscription Information.	Contract, Legal Obligation.

18	Mergers, Acquisitions, Corporate Restructuring	Customer Records, Employee Data, Vendor Information.	Legal Obligation.

7. Consent

Where processing of Personal Data is based on consent, Union bank shall obtain the requisite consent of Data Subjects at the time of collection of Personal Data. In this regard, Union bank will ensure:

a) that the specific purpose of collection is made known to the Data Subject and the Consent is requested in a clear and plain language;
b) that the Consent is freely given by the Data Subject and obtained without fraud, coercion or undue influence;
c) that the Consent is sufficiently distinct from other matters to which the Data Subject has agreed;
d) that the Consent is explicitly provided in an affirmative manner;
e) that Consent is obtained for each purpose of Personal Data collection and processing; and
f) that it is clearly communicated to and understood by Data Subjects that they can update, manage or withdraw their Consent at any time.

7.1 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, preticked boxes or inactivity does not constitute Consent under the NDPA/GAID.

Consent in respect of Sensitive Personal Data must be explicit. A tick of the box would not suffice.

7.2 Processing of Personal Data for Accounts held by Minors

Union Bank recognises the special protection afforded to children and individuals lacking legal capacity under the NDPA. Section 31 of the Act expressly requires that their personal data be processed only where appropriate consent is provided by a parent or legal guardian.

Accordingly, when a Minor's account is opened or maintained under parental or guardian supervision, the Bank shall ensure that:

1. **Parental or Guardian Consent is Mandatory:**

The Bank obtains verifiable consent from the parent or legal guardian before collecting, using, or processing the child's personal data. The GAID provides operational clarity that valid consent must be freely given, specific, informed, and meet heightened scrutiny when processing children's data.

2. **Limited and Necessary Data Processing:**
   Only personal data required to establish and manage the Minor's account, and to comply with applicable legal and regulatory requirements, will be collected.

3. **Age-Appropriate Safeguards:**
   The Bank applies enhanced safeguards for Minor accounts, including:

   - strict access controls
   - reduced data retention periods
   - heightened transparency obligations toward parents/guardians

4. **Right to Withdraw Consent:**
   Parents or legal guardians may withdraw consent at any time, in accordance with data subject rights under the NDPA.

5. **No Automated Decision-Making:**
   Children's data is not subject to automated decision-making processes that may significantly affect the child, consistent with the heightened duty of care mandated under the GAID.

The Bank does **not** process minors' data for marketing, profiling, or purposes unrelated to account management or statutory obligations.

7.3. **Processing of Personal Accounts for Politically Exposed Persons (PEPs)**

Processing of Politically Exposed Persons (PEPs) data is carried out under contractual basis and legal obligations arising from AML/CFT regulations. In line with NDPA principles and GAID guidance, such processing is treated as high-risk, requiring enhanced safeguards and a Data Protection Impact Assessment (DPIA).

Additional safeguards may include;

1. **Enhanced Identity Verification**:
   The Bank conducts additional checks to verify the identity and political exposure status of the customer, applying greater scrutiny than for standard customers.

2. **Risk-Based Monitoring:**
   Personal data of PEPs may be subject to enhanced monitoring to comply with regulatory and anti-financial-crime obligations, strictly in accordance with the principles of necessity, proportionality, and purpose limitation.

3. **Minimal and Purpose-Specific Processing:**

Only personal data required to meet statutory Know-Your-Customer (KYC) and Anti-Money Laundering (AML) obligations will be processed.

4. **Access Controls:**
   PEP data is accessible strictly on a need-to-know basis and protected with strengthened administrative and technical controls in accordance with the Bank's duty to maintain confidentiality and integrity of personal data.

The Bank does not use PEP classification for profiling unrelated to regulatory requirements.

8. Data Subject Rights

8.1 All individuals who are the subject of Personal Data held by Union bank are entitled to the following rights:

a) Right to request for and access their Personal Data collected and stored. Where data is held electronically in a structured form, such as in a Database, the Data Subject has a right to receive that data in a common electronic format;
b) Right to information on their personal data collected and stored;
c) Right to objection or request for restriction;
d) Right to object to automated decision making;
e) Right to request rectification and modification of their data which Union bank keeps;
f) Right to request for deletion of their data, except as restricted by law or Union bank's statutory obligations;
g) Right to request the movement of data from Union bank to a Third Party; this is the right to the portability of data;
h) Right to object to, and to request that Union bank restricts the processing of their information except as required by law or Union bank's statutory obligations; and
i) Right to lodge a complaint with the NDPC.

To opt out of marketing and unsolicited messages:

If you no longer want to receive marketing messages from Union bank, you can choose to opt out at any time. If you've previously opted in to receive personalized content based on how and where you use our network, you can also opt out at any time.

These are various ways to opt out:

- Contact our customer services team – see the contact us page Here https://www.unionbankng.com/contact-us/
- Click the unsubscribe icon from our email; and

- Disable push notification messages, including marketing messages, at any time in our apps by changing the notification settings on your device or by uninstalling the app.

8.2 Union bank well-defined procedure regarding how to handle and answer Data Subject's requests are contained in Union bank's Data Subject Access Request Policy.

Data Subjects can exercise any of their rights by completing Union bank's Subject Access Request (SAR) Form and submitting to Union bank via dpo@unionbankng.com

8.3 Data Subject Authentication Requirements

Before responding to any Data Subject request, Union bank shall authenticate the identity of the requester through reasonable verification methods, including:

- Confirming account identifiers
- Matching registered phone number or email
- Requesting additional verification documents where needed

Union bank shall refuse or delay processing where identity cannot be reasonably confirmed.

Automated Decision-Making & Profiling

9. Transfer of Personal data

9.1 Third Party Processor within Nigeria

Union bank may engage the services of third parties in order to process your Personal Data by collected by us. The processing by such third parties shall be governed by a written contract with Union bank to ensure adequate protection and security measures are put in place by the third party for the protection of Personal Data in accordance with the terms of this Policy, the NDPA and GAID We may also share your personal data with law enforcement agencies where required by law to do so.

Where applicable, Union bank will share your information with:

a) Partners, suppliers or agents involved in delivering the products and services you have ordered or used.

b) Law enforcement agencies, government bodies, regulatory organizations, courts or other public authorities if we have to, or are authorized to by law.

c) A third party or body where such disclosure is required to satisfy any applicable law, or other legal or regulatory requirement e.g. to detect or prevent fraud or Union bank of any other crime.

d) A merging or acquiring entity where we undergo business reorganization e.g. merger, acquisition or takeover.

9.2 Transfer of Personal Data to Foreign Country

9.2.1 Where Personal Data is to be transferred to a country outside Nigeria, Union bank shall put adequate measures in place to ensure the security of such Personal Data. In particular, Union bank shall, among other things, conduct a detailed assessment of whether the said recipient of the personal data is subject to a law, binding corporate rules, contractual clauses, code of conduct or certification mechanism that affords an adequate level of protection with respect to the personal date in accordance with **Section 41 of the NDPA, and Schedule 5, Paragraph 2 of the GAID.**

9.2.2 Union bank shall record the basis for transfer of personal data to the recipient of the personal data under Paragraph 8.2.1 and the adequacy of protection stated in **Section 42 of the NDPA and Schedule 5, Paragraph 2 of the GAID**.

9.2.3 Where Union bank is unable to transfer Personal Data to a country outside Nigeria in accordance with Paragraph 8.2.1 above, Union bank will transfer such Personal Data out of Nigeria under one of the following conditions:

a. The consent of the Data Subject has been obtained;

b. The transfer is necessary for the performance of a contract between Union bank and the Data Subject or implementation of pre-contractual measures taken at the Data Subject's request;

c. The transfer is necessary for the sole benefit of a Data Subject and:

i. it is not reasonably practicable to obtain the consent of the Data Subject to that transfer, and ii. if it were reasonably practicable to obtain such consent, the Data Subject would likely give it.

d. The transfer is necessary for reason of public interest;

e. The transfer is for the establishment, exercise or defense of legal claims;

f. The transfer is necessary in order to protect the vital interests of the Data Subjects or other persons, where the Data Subject is physically or legally incapable of giving consent.

Provided, in all circumstances, that the Data Subject has been manifestly made to understand through clear warnings of the specific principle(s) of data protection that are likely to be violated in the event of transfer to a third country, this proviso shall not apply to any instance where the Data Subject is answerable in duly established legal action for any civil or criminal claim in a third country.

Union bank will take all necessary steps to ensure that the Personal Data is transmitted in a safe and secure manner. Details of the protection given to your information when it is transferred outside Nigeria shall be provided to you upon request.

9.3 Third-Party Risk Management Requirements

To ensure security when Personal Data is handled by external partners:

- All third parties processing Personal Data on behalf of Union Bank must sign a **Data Processing Agreement (DPA)**.
- Third parties must demonstrate adequate data protection controls, including encryption, access management, and breach procedures.
- Annual compliance reviews shall be performed on third parties handling Sensitive Personal Data.
- Cross-border processors must meet NDPA adequacy standards.
- Immediate notification must be provided to Union bank for any suspected or actual data breach.

10. Data Breach Management Procedure

10.1 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.

10.2 All employees must inform their designated line manager or the Data Protection Officer of Union bank immediately about cases of violations of this Policy or other regulations on the protection of Personal Data, in accordance with Union bank'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) cyber-attacks.

10.3 A data protection breach notification must be made immediately after any data breach to ensure that:

a) immediate remedial steps can be taken in respect of the breach;
b) any reporting duties to Nigeria Data Protection Commission (NDPC) or any other regulatory authority can be complied with,
c) any affected Data Subject can be informed and

d) any stakeholder communication can be managed.

10.4 When a potential breach has occurred, Union bank 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.
g) Ensure that impacted Data Subjects are properly notified, if necessary.

10.5 You can read more about Union bank's Personal Data Breach Management Procedure by requesting a copy via dpo@unionbankng.com

11. Data Protection Impact Assessment

Union bank 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 freedoms of the Data Subject in accordance with Articles 28 and 13, Paragraph 5 (e) of the GAID.

Union bank shall document the DPIA in line with the template provided for in Schedule 4 of the GAID and shall carry out the DPIA in line with the procedures laid down in Union bank's **Data Protection Impact Assessment Policy.**

12. Data Security

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

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

a) Industry-accepted hardening standards, for workstations, servers, and databases.

b) Full disk software encryption on all corporate workstation/laptop operating systems drives storing Personal and Personal/Sensitive Data.
c) Encryption at rest including key management of key databases.
d) Enable Security Audit Logging across all systems managing Personal Data.
e) Restrict the use of removable media such as USB flash disk drives.
f) Anonymization techniques on testing environments.
g) Physical access control where Personal Data is stored in hardcopy.

12.3 Personal data is classified as confidential by definition. Union bank shall respect the confidentiality of personal data at all times during processing. Personal data shall be filed and stored in a way that only authorized personnel can have access to the data. Personal data shall also be transferred using secured and reliable means of communication.

12.4 Union Bank shall take necessary and appropriate measures to protect personal data from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data. All security measures shall be in accordance with Union Bank Information Security Policy. Union bank shall continuously assess and implement a high level of data security that is appropriate for the risk associated with processing of personal data.

13. Data Protection Officer

Union bank shall appoint a Data Protection Officer(s) (DPO) responsible for overseeing Union bank's data protection strategy and its implementation to ensure compliance with the NDPA/GAID requirements. The DPO shall be a knowledgeable person on data privacy and protection principles and shall be familiar with the provisions of the NDPA/GAID.

The DPO shall be a person who is assessed in line with the parameters in Schedule 3 of the GAID.

The main tasks of the DPO include:

a) administering data protection policies and practices of Union bank;
b) monitoring compliance with the NDPA/GAID and other data protection laws, data protection policies, awareness-raising, training, and audits;
c) advice the business, management, employees and third parties who carry on processing activities of their obligations under the NDPA/GAID;
d) acts as a contact point for Union bank;
e) monitor and update the implementation of the data protection policies and practices of
Union bank and ensure compliance amongst all employees of Union bank;
f) ensure that a semi-annual Data Protection audit report is submitted to the Management of Union bank;

g) ensure that he/she vets and signs DPIAs upon completion;
h) ensure that Union bank undertakes a Data Impact Assessment and curb potential risk in Union bank data processing operations; and
i) maintain a database of all Union bank data collection and processing operations of Union bank.

14. Training

Union bank 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, the NDPA/GAID with regard to the *protection* of Personal *Data*. On an annual basis, Union bank shall develop a capacity building plan for its employees on data privacy and protection in line with the NDPA and GAID

15. Data Protection Audit

Union bank shall conduct an annual data protection audit through a licensed Data Protection Compliance Organization (DPCOs) to verify Union bank's compliance with the provisions of the NDPA/GAID and other applicable data protection laws.

The audit report will be certified and filed by the DPCO to the NDPC as required under the NDPA and GAID

16. Related Policies and Procedures

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

- Personal Data Breach Management Policy
- Information Security Policy (Information Security Policy - Union Bank of Nigeria)
- Document Retention Policy
- Cookies Policy (Cookie Policy - Union Bank of Nigeria)
- Privacy Notice (Privacy Policy - Union Bank of Nigeria)
- Data Protection Impact Assessment Procedure

17. Changes to the Policy

Union bank reserves the right to change, amend or alter this Policy at any point in time. If we amend this Policy, we will provide you with the updated version.

18. Policy Enforcement & Disciplinary Measures

Union Bank maintains a zero-tolerance stance for the unlawful disclosure or mishandling of Personal Data.

Union bank ensures that employees, contractors, and third-party partners who process Personal Data on behalf of Union bank are held accountable in line with applicable legal, regulatory, and contractual obligations. Appropriate remedial or administrative actions shall be taken for violations.

19. Glossary

"Consent"	means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, through a statement or a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her.
"Database"	means a collection of data organized in a manner that allows access, retrieval, deletion and processing of that data; it includes but not limited to structured, unstructured, cached and file system type Databases.
"Data Processor	means a person or organization that processes Personal Data on behalf and on instructions of Union bank.
"DPCO"	means an organization registered by NDPC to provide data protection audit, compliance and training services to public and private organizations who process Personal Data in Nigeria.
"Data Subject"	means any person, who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
"NDPA"	means the Nigeria Data Protection Act, 2023.
GAID'	means General Application and Implementation Directive, 2025.
"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, 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.