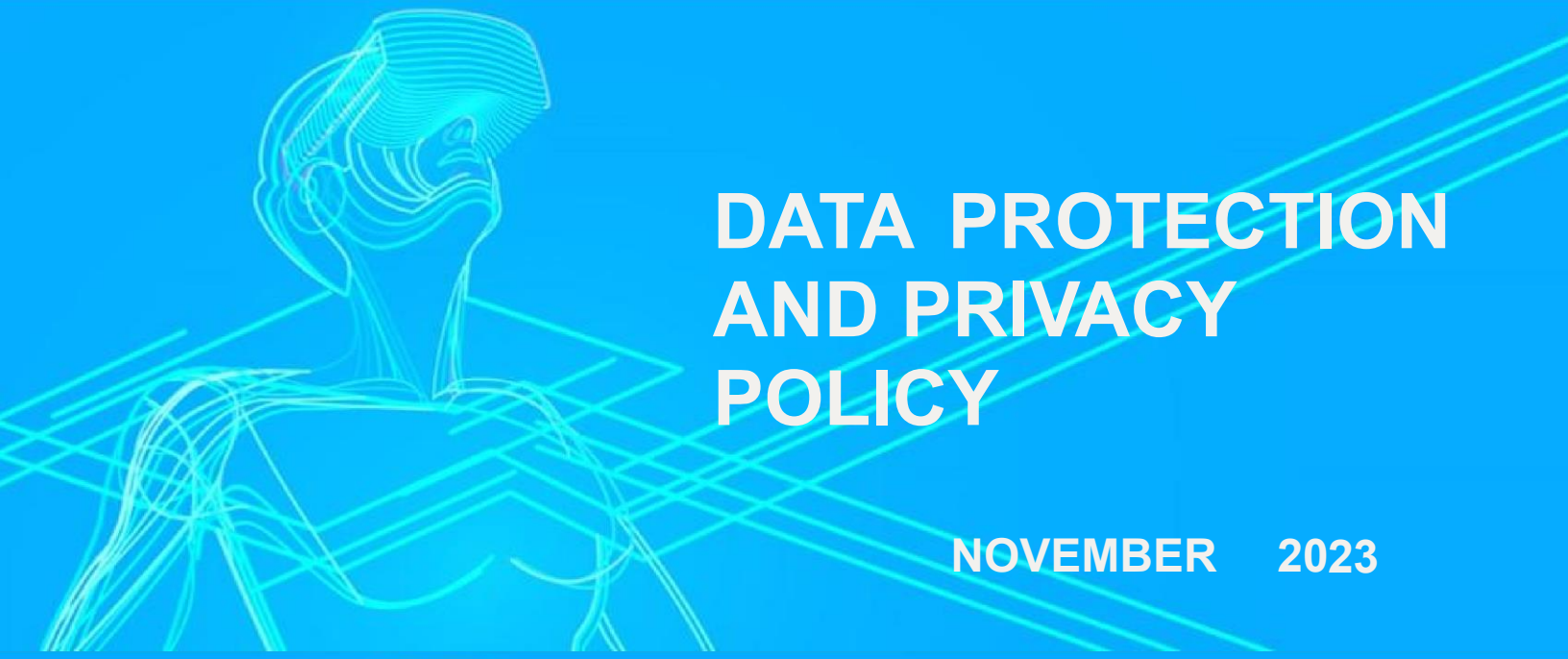
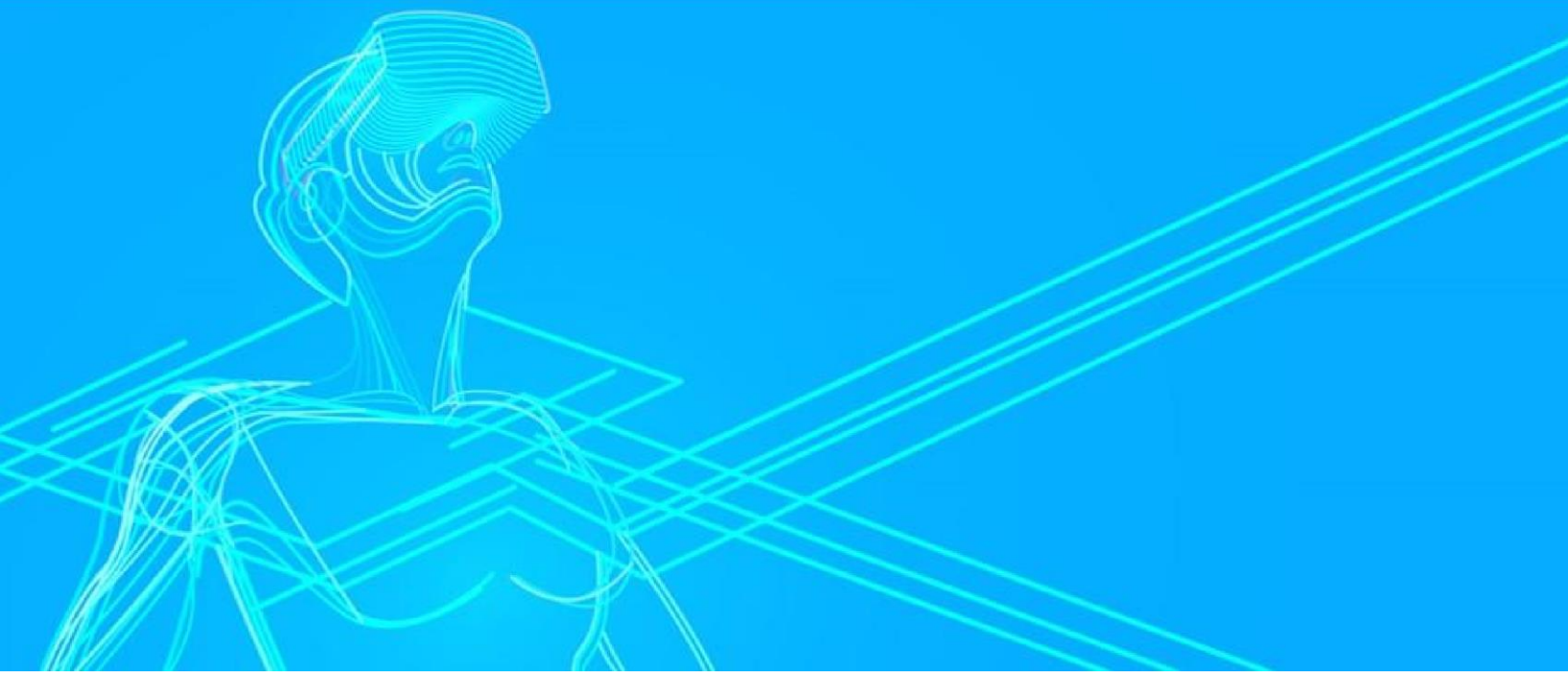
unionbank



DATA PROTECTION AND PRIVACY POLICY

NOVEMBER 2023



Document Management Information

Document Title: Data Protection & Privacy Policy -UBN Information Security 2023

Document Status: Approved

Issue Details

Release Date	

Revision Details

Version No.	Revision Date	Particulars	Approved by
1.0	June 2020	Initial Documentation	
2.0	June 2021	Annual Review	
3.0	June 2022	Annual Review	
4.0	November 2023	Incorporated "legitimate interest" as one of the legal basis of processing data in line with the Nigeria Data Protection Act 2023. Change NITDA to NDPC Data Protection Officer changed from Lateef Dabiri to Francis Mojoyinlola	

Document Contact Details

Role	Name	Designation
Author	Opeoluwa Ogundipe	Information Security
Reviewer/ Custodian	Kingsley Duru	Team Lead, Cyber Governance, Risk & Compliance
Owner	Francis Mojoyinola	Chief Information Security Officer/DPO

Distribution List

Name

Information Security

Reference Documents

Document Name	Document Number	Version No.
Data Protection & Privacy Policy	DOC/NDPR/060	4.0

Contents

1.0 INTRODUCTION

Union Bank of Nigeria Plc. (Union Bank or UBN), founded in 1917 is one of Nigeria's most recognized and respected Banks. UBN is a large commercial Bank, serving individuals, small and medium-sized companies, as well as large corporations and organizations through a nationwide platform of over 270 branches with staff committed to delivering top-notch financial services to our customers and ensuring they enjoy safe and secure Banking through all our platforms.

UBN processes data and information inter alia, to:

- Deliver and market services to customers;
- Fulfill legal and contractual obligations
- Exercise responsibilities and duties as an employer;
- Protect the legitimate interest of bank, data subject(s), staff and third parties.

In the course of the bank's business, it may be necessary to share data with external service providers, business partners, third parties and customers on a need to know basis through various methods such as, but not limited to, email, telephone, fax, approved cloud-based solutions etc. Data may also be required to be transferred to another country.

As a data controller UBN has a duty to ensure that it safeguards data against breach of privacy, loss, damage, unlawful access and unauthorized destruction.

A data privacy breach or loss, whether accidental or deliberate, presents significant legal, financial and reputational risks to the bank.

In order to manage these risks and to protect our employees, customers and third parties this policy sets out rules and responsibilities for processing data for and on behalf of UBN.

2.0 PURPOSE

This policy describes how UBN store, handle and secure personal data, fairly, transparently, and with confidentiality. The purpose is to ensure that we process personal data in a way and manner that is consistent with the Nigeria Data Protection Act (NDPA) 2023 and other relevant data protection practices and guidelines.

3.0 DATA PRIVACY COMMITTMENT 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.
- That breaches of data privacy, actual or suspected, are reported to be investigated by UBN
- The maintenance of our ISO 27001 certification.

The regulatory body, Nigeria Data Protection Commission (NDPC), with the statutory mandate for compliance with the NDPR, has defined huge fines for the bank for data breaches and noncompliance with the regulation.

4.0 APPLICATION AND SCOPE (ROLES AND RESPONSIBILITIES)

- The Bank has appointed a data protection officer (DPO) whose primary role is to ensure that the bank processes the personal data of staff, customers, providers or any other individuals (also referred to as data subjects) in compliance with the applicable data protection and privacy rules.
- The Policy governs the roles and responsibilities of everyone who processes data in: (a) The course of their work with UBN
  (b) Providing services for or on behalf of UBN.
- This policy applies to all personal data held by Union Bank for customers, vendors, suppliers, employees etc.
- This policy applies irrespective of the UBN premises where the data processing takes place i.e. within one Union Bank office, between different Union Bank offices in the same or across multiple jurisdictions.
- This policy applies to data transferred to third parties.
- This policy continues to apply even after data subjects no longer have a relationship with Union Bank but the bank still has access to the personal data.
- Compliance with this policy is mandatory for all Union Bank staff with access to personal data at the bank

5.0 FREQUENTLY USED WORDS IN THE POLICY AND THEIR DEFINITION

For the purpose of this policy, the following definitions apply;

5.1 Personal data

This is 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 and others.

5.2 Data subject(s)

This is an identifiable person; one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

5.3 Consent

Any freely given and informed indication of an agreement by the data subject to the processing of his/her personal data, which may be given either by a written or oral statement or by a clear affirmative action.

5.4 Data Controller

A data controller is any person who either alone, jointly with other persons or in common with other persons or as a statutory body determines the purposes for and the manner in which personal data is processed or is to be processed.

5.5 Data Protection Officer (DPO)

The DPO's responsibility is to ensure that the bank is correctly protecting individuals' personal data according to the subsisting data protection and privacy legislation.

UBN's DPO is Francis Mojoyinola, and his responsibilities include ensuring the bank's compliance with the NDPR, liaising with customers and employees on privacy-related requests, liaising with data protection authorities, and keeping our staff informed of updates to data protection and privacy requirements.

5.6 Data Processing

This includes but not limited to actions taken to obtain, record, store, share, use, destroy or analyse data.

5.7 Data transfer agreement

An agreement between Union Bank and a partner or third party that states the terms and conditions of use of personal data, including which data components are to be shared, the mode of transfer, how the data may be used, data security measures and other related issues.

5.8 Personal data breach

A breach of data security leading to the unlawful/ illegitimate disclosure, loss, alteration, unauthorized access to personal data transferred, stored or otherwise processed.

5.9 Third party

Any legal person or body other than the data subject or Union Bank. Examples of third parties are national governments, international governmental or non-governmental organizations, private sector entities or individuals.

6.0 BASIC PRINCIPLES OF PERSONAL DATA PROCESSING

The general rule to follow by all staff is to process information as carefully as you would wish data about yourself to be processed. The conditions and principles for data processing that follow below, are an expansion of this rule -

6.1 Process data fairly and lawfully:

Personal data shall be processed on a legitimate basis and in a fair and transparent manner. The bank will only process personal data based on one or more of the following;

- With the consent of the data subject, which must align with the provision of section 2.3 of the NDPR.

- In the best interest of the data subject
- To enable the bank, perform its operation

We shall also:

- Comply with the provisions of this policy document and any applicable regulations, statutes, and contractual obligations with reference to the processing of data as communicated from time to time.
- Process data taking the interests of the data subject(s) into consideration as to not infringe rights to privacy.

If you receive an objection to the processing of information or a request for access to data – contact your Data Protection Officer to assist.

6.2 Keep the data processed relevant to a specific purpose and to a minimum:

We shall only process personal data in a way that is compatible with the purpose for which it has been collected or subsequently authorized by the data subject. We shall also:

- Only process data relevant to the specific purpose(s) it is collected for.
- Obtain voluntary consent from the data subject(s) for processing information. (UBN template employment contracts and customer account opening forms contain general consent provisions- but determine upfront whether these are sufficient for your purpose. Consult the DPO if you require further assistance.)
- Compulsorily obtain voluntary consent from the legal representative or legal guardian of data subject(s) for processing personal data on children younger than 18 years.
- Data may be processed without consent in the following circumstances:
    a. Processing is necessary for the establishment, exercise, defense, or compliance of a right or obligation in law;
    b. Processing is to protect the vital interests of the data subject or a third party;
    c. Processing is done for historical, statistical or research purposes; d. .

6.3 Collect the data directly from the data subject – unless the following exceptions apply:

- The data is contained in a public record;
- The data subject(s) has deliberately made the information public;
- The data subject(s) has consented to the collection of the information from another source;
- The privacy interests of the data subject(s) are not prejudiced;
- Collection from another source is necessary to avoid prejudice of the maintenance or enforcement of a law, court proceedings, interests of national security or legitimate interests of a processor that determines the purpose and means of processing the data.

6.4 Always maintain the confidentiality of personal data:

Personal data is classified as confidential by definition. The 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.

6.5 Take appropriate measures to secure personal data:

- 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. This aligns with section 10 of the NDPR.
- The bank shall continuously assess and implement a high level of data security that is appropriate for the risk associated with processing of personal data.
- Data owners shall take reasonable steps to confirm that data controlled by departing employees is appropriately transitioned in order to support business continuity.

Union Bank shall implement organizational and technical measures to ensure that the data processing meets the requirements of this policy.

- This organizational measure includes;
  Training staff on data protection and security
  Conducting data protection and privacy impact assessment

- Technical measures include**;**
  Ensuring compliance to relevant Union Bank IT polices and security

- Union Bank's Information Security team shall be responsible for defining and maintaining the processes and supporting standards that relate to providing existing Union Bank employees with access to critical data or data controlled by departed or departing employees. The Information Security team shall consult with Union Bank's Legal Department, Human Resources, Data and Analytics Office, Internal Audit, and Technology teams to develop, maintain, and implement these processes as needed.
- All business process that uses, accepts, stores, or transmits personal data shall have a process in place to protect and safeguard the data from unauthorized disclosure and ensure that its usage is consistent with existing privacy policies and legal requirements. This aligns with section 2.1(2) of the NDPR.

6.6 Limit the retention of data:

- Don't retain data for any longer than is necessary for achieving the purpose it was processed for, this aligns with section 2.1(1) c of Nigeria Data Protection Regulation
- Ensure however that your retention period is in compliance with legislative requirements and Union Bank's Document Retention Policy – contact the Data Protection Officer should you require clarity on this.

6.7 Take steps to ensure the quality and accuracy of data:

Personal data must always be accurate, reliable, current and relevant to its intended use and there are no omissions during data processing. This aligns with section 2.1(3) of the NDPR. .
We shall also:

- Take reasonable steps to determine that the data processed is complete, accurate, not misleading and up to date.
- If the data subject(s) request any information to be corrected – investigate the request and respond thereto. If in disagreement with the request – link the request with the data to ensure that it will be read with an indication that the information is disputed but not changed. Where changes are made that might impact decisions made on data processed prior to the change – parties that may have taken such decisions must be notified of the changes.

6.8 Further processing of data shall be limited:

Limit further processing of data to comply with the purpose for which it was initially processed – unless further processing was agreed to by the data subject, can be implied through contractual provisions with the data subject or are justified for legal /security or other legitimate purposes.

6.9 Notify the data subject of the processing of information:

Data subjects shall be informed of the privacy policies that applies to their data, this shall be communicated via all medium through which data is collected and processed. The information should include:

- Purpose for data collection
- Description of data to be collected
- Content of the data subjects' consent
- How data is collected and stored
- Remedies for data violation and the timelines
- Whether data will be transferred to third parties for any reason
- Any consequences for refusing or failing to provide the requested personal data, and the importance of providing an accurate and complete data
- Data subjects right to request for access to their personal data for review, correction or deletion
- The right to lodge a complaint with the appropriate authorities.

This aligns with section 2.13.6 of the NDPR on Rights of Data subject.

We shall also:

- Ensure that the template employment and customer forms contain general consent provisions that cover the requirements of this principle.
- Determine on a case by case basis whether these general provisions could be relied upon to infer or reasonably assume that the data subject(s) are aware of the processing. Consult the Data Protection Officer if you require further clarification.

6.10 Legal Grounds for Processing of Personal Data

In line with the provisions of the NDPR, processing of Personal Data by Union Bank shall be lawful if at least one of the following applies:

a) the Data Subject has given Consent to the processing of his/her Personal Data for one or more specific purposes;

b) 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, and

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.

f) processing is necessary for the purposes of the legitimate interests pursued by the bank or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This is a new introduction of Section 25(1)(v) of the Data Protection Act 2023.

g) The Act introduces legitimate interest of a data controller as one of the lawful bases for processing personal data. However, "legitimate interest" will not be a basis for processing personal data where such interests are overridden by the data subject's fundamental rights and freedom or are incompatible with the other lawful bases or the data subject would not have a reasonable expectation that the personal data would be processed in the manner envisaged. This is the balancing test for determining "legitimate interest"

.

6.11 Data Subject Rights

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; and

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.

- Union Bank's well-defined procedure regarding how to handle and answer Data Subject's requests including the appropriate situations for withholding of information are contained in Union Bank's Data Subject Access Request Policy.

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

6.12 Transfer of personal data to third party shall be well governed and managed:

In cases where, the collection and/or processing of personal data is done by a third party on behalf of the bank, the third party is expected to respect and implement the same or basic principles of personal data privacy and protection as contained in this policy.
Union Bank shall strive to take reasonable and appropriate steps on processes listed below:

- ***Third Party Data Processing Contract***

The bank shall seek to sign a Third-Party Data Processing Contract with the third party. The Third-Party Data Processing Contract shall include:

- The purpose(s) for data transfer, and the data protection and the security measures to be put in place.
- A requirement for the third party to comply with the data protection privacy and security measures in this policy. Consider the inclusion of a "right to audit" clause to permit the bank ensure the data privacy rights of data subjects is upheld.

- ***Policy verification*** ○ Establish that the third party operates same data protection standard and basic principles as the bank.
  - ○ Ensure that the third party effectively processes the personal data in a manner consistent with its obligations under this Policy.

- ***Transfer of personal data to third party*** ○ Transfer such personal data only for specified purposes and limit the third party's use of the data to the specified purposes.
  - The bank shall ensure that the third party maintains high level of data security and protection for personal data against the risk of loss, alteration, destruction etc. ○ The third party respects the confidentiality of personal data transferred to them and are obligated to provide the same level of privacy protection as is required by this policy through a written contract.
  - Ensure that the third party effectively processes the personal data in a manner consistent with its obligations under this policy.

- ***Contract termination***

  Upon termination of the contract, all personal data collected during the partnership must be returned to the bank, unless otherwise where an exception exists due to legitimate or regulatory reasons.

  The bank shall also require the third party to notify the bank if the third party determines it can no longer meet its obligation to provide the same level of protection as is required by this policy, and upon notice from a third party, take further steps to immediately stop and remediate any unauthorized processing.

6.13 **Transfer of Personal Data Outside Nigeria**

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. Union Bank shall, among other things, conduct a detailed assessment of whether the said country is on the NDPC's White List of Countries with adequate data protection laws.

Transfer of Personal Data out of Nigeria would be in accordance with the provisions of the NDPR and the Nigeria Data Protection Act (NDPA). Union Bank will therefore only transfer Personal Data out of Nigeria on 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 to conclude a contract between Union Bank and a third party in the interest of the Data Subject;

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.

Where the recipient country is not on the White List and none of the conditions listed above is met, Union Bank will engage with NITDA and the Office of the Honourable Attorney General of the Federation (HAGF) for approval with respect to such transfer.

6.14 Data Breach Management Procedure

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

- All employees must inform their designated line manager or the DPO 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) human error resulting in data being shared with someone who does not have a right to know; and

f) hacking attack.

• A data protection breach notification must be made in real time after any data breach to ensure that:

a) immediate remedial steps can be taken in respect of the breach;

b) any reporting duties to 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.

• 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.

6.15 You can read more about Union Bank's Personal Data Breach Management Procedure via the attached embedded below.

Union Bank - Data Breach Management P

7.0 E-LEARNING AND NOTIFICATIONS ON DATA PROTECTION AND PRIVACY

As a staff of the bank, you are responsible to ensure that you read, comply with and remain informed about UBN's data privacy policies and procedures and to complete all mandatory training and e-learning courses related to data protection by the dates prescribed by UBN.

8.0 MARKETING TO CUSTOMERS OR PROSPECTIVE CUSTOMERS

Authorised electronic marketing to customers or prospective customers must contain an 'opt out' (unsubscribe option).

In the event that the recipient selects the unsubscribed option, this shall be recorded, and no further marketing material shall be sent to such recipient.

9.0 CAMERA AND SOUND RECORDINGS

The use of picture and/or sound recording functionality in devices is subject to the rights of privacy of individuals and subject to confidentiality obligations towards customers, employees and other parties. This means that it is not permitted to take pictures or record conservations of other employees, suppliers or customers without their express or implied consent- unless such a recording or picture is in the legitimate interest of UBN (e.g. to identify theft or fraud, or for disciplinary or grievance proceedings, security, etc.)

Under no circumstance may photos or video recordings be taken of UBN sensitive or restricted zones (server, hub, security, filing rooms, etc.) without the consent of Corporate Security.

10.0 ACCESS AND CORRECTION OF PERSONAL DATA

The data subject has a right to request for information on the personal data being processed, the purpose(s) for processing such data and the third parties to whom such data has been or is being or will be transferred.
Data subjects may also request access to their personal data for purposes of correcting, amending or deleting information where it is inaccurate, incomplete, unnecessary or excessive. This aligns with section 2.13.8 NDPR Rights of Data Subject

In addition:

- Data subjects are entitled to request access to information processed by UBN and where such information is incorrect, the data subject(s) may request the incorrect information be corrected. (Sufficient proof may be required from the data subject prior to correction of the information).
- All requests for access to information by data subjects must be submitted in writing. For staff personal data request UBN employees must submit such written requests through their respective HRBP's – HR business partners who will channel this to the DPO.
- Request for data by third parties or former employees, shall be addressed in writing to HR and managed by the HR business partners who will channel this to the DPO.

10.1 Modalities of Requests

The bank shall confirm the identity of the person making a request before complying with the request. Each data subject is required to identify himself/herself in an appropriate manner. Where the available means of identity is not enough, additional information shall be requested from the data subject. In the case of a legal representative or legal guardian, proof of such legal authority needs to be supplied. Requests and objections from parents or guardians for children shall be evaluated against the best interests of the child. This aligns with section 2.13.4 of Nigeria Data Protection Regulation 2019 Procuring Consent.

Data subjects may make request for information about access to, correction, deletion or objection to personal data processing. An authorized legal representative and a parent in the case of a child

can also make this request. All request can be made in writing, orally or electronically to the office where data is being processed.

Union Bank undertakes that, where there is reasonable cause for appropriate withholding of personal data upon Data Subject request, we shall inform the Data Subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with NDPR, provided that there is no other law or regulation that precludes us from providing such information to the Data Subject.

To the extent permitted by applicable laws, Union Bank may refuse to act on a Data Subject's request, if at least one of the following applies:

a) in compliance with a legal obligation to which Union Bank is subject;
b) protecting the vital interests of the Data Subject or of another natural person; and
c) for public interest or in exercise of official public mandate vested in Union Bank.

You can read more about the Data subject access request policy via the attached embedded below:

Union Bank- Data Subject Access Reque

10.2 Recording and Response

The bank shall act on request from data subjects within a reasonable time, in writing or orally, and in a language, that is understandable to the data subject and/or his or her legal representative or legal guardian, as applicable and where there is a delay, communication shall be sent to the Data subject on reasons for the delay. This align with Sections 2.13.2 and 2.13.3 of NDPR.

11.0 AUDIT

In line with section 3.1.7 of NDPR implementation mechanism, Union Bank shall ensure compliance to the data protection audit requirements and expectations.

Accordingly, UBN shall procure the services of a competent DPCO to support in monitoring, auditing, training and data protection compliance consulting in line with the NDPR requirements.

Data management controls in designated data systems may be audited in accordance with Union Bank audit processes and NDPR data protection audit. Where controls are not automated in the system, such controls must be assessed, at least annually, as a component of an audit of the environment and all data privacy and protection policies may be audited as well.

Where a new system is to be implemented, the new system shall be assessed for design and implementation of data management controls. Where a new system is to be implemented, and the new system collects, uses, accesses, analyses, stores, transfers, or destroys personal data, the new system needs to be assessed for privacy concerns and control implementation.

12.0 COMPLIANCE WITH THE PROVISION OF THIS POLICY

- Take note that staff shall be measured in terms of your adherence to UBN's data privacy and protection requirements. Your adherence to such requirements forms part of your performance outcomes.
- Any non-compliance with this policy provisions will result in the application of UBN Disciplinary Sanction Measures. Violation of this Policy by an employee, a third party or contractor of Union Bank shall result in appropriate discipline up to and including termination.

13.0 LEGAL AND REGULATORY CONSIDERATION

This policy is aligned with all the various applicable data protection laws and therefore compliance with this policy will support compliance with such legislation. In the event that there are stricter requirements imposed in a specific jurisdiction, the stricter requirements must be adhered to.

14.0 EXCEPTION TO POLICY PROVISIONS

All requests for exceptions to this policy shall be documented and, approved by the DPO (or equivalent as applicable).

15.0 REVIEWS OF POLICY

UBN reserves the right to review, re-evaluate and amend this policy at any time.