DATA PRIVACY NOTICE FOR CURRENT/PAST EMPLOYEES AND RECRUITEMENT CANDIDATES

Date Created	28/08/2024
Document Author	Data Protection Officer
Document Owner	Fidelity Bank
Date Reviewed	6th August 2025
Document Classification	Public

Version 1.1

Document Control Sheet Version and Update History

Version	Date	Author	Change from Previous Version
Version 1.0	1st August 2023	Data Protection Officer	Nil
Version 1.1	28th August 2024	Data Protection Officer	• Update of the DPO to Jude C. Ike- Muonso
Version 1.2	6th August 2025	Data Protection Officer	• Changed the DPO • Changed no 3 to Legal basis for data processing • Made the document concise compared to the previous version. • Corrected typographical errors.

Contents

1. INTRODUCTION

Fidelity Bank Plc is a bank licensed in Nigeria by the Central Bank of Nigeria. We provide banking services to a wide variety of customers including individuals, small and medium enterprises, large corporates and multinationals, governmental institutions, and non-governmental institutions. Our banking services are provided at our branches and through e-channels including the Internet.

Data privacy is taken very seriously at the Bank. We respect the privacy rights of our customers, employees, vendors, and every other category of individuals whose data we come across. The Bank is always dedicated to handling personal data responsibly and in accordance with all applicable laws. We deem it necessary that you know what we do with the personal information that we request from you, why we request such information and what we do with them. This document outlines our approach to Data Protection and Privacy to fulfil our obligations under the Nigeria Data Protection Act (2023), as well as other applicable laws/regulations.

This Privacy Notice outlines how we collect, process, use, store, and disclose personal data relating to:

- Job candidates
- Prospective employees
- Current employees (including outsourced staff)
- Former employees

This Notice also outlines your rights as a Data Subject, as well as your obligations in safeguarding personal data you may access by virtue of your relationship with the Bank.

Processing activities are conducted under one or more of the lawful bases defined in the NDPA 2023, including: consent, performance of a contract, legal obligation, legitimate interest, vital interest, and the performance of a public task.

This Notice should be read in conjunction with Fidelity Bank's Data Protection and Privacy Policy and other relevant internal policies.

2. WHEN AND HOW WE COLLECT INFORMATION ABOUT YOU

We collect personal data at various stages of your engagement with the Bank, including:

- During the recruitment and application process
- Upon acceptance of an employment offer
- During the course of your employment
- After employment ends (for statutory or administrative purposes)

We may also collect data from third-party sources such as background verification agencies, educational institutions, references, and regulatory bodies.

3. Legal Basis For Processing By Category Of Data Subject

We process different categories of personal data depending on your relationship with the Bank:

- **Employees and Outsourced Staff**: We process your personal data primarily to fulfil our contractual obligations to you, manage the employment relationship effectively, and ensure proper profiling on our internal systems. This enables us to provide you with the tools, systems, and resources required to perform your job functions.
- **Former Employees**: We retain and process your personal data to comply with legal and regulatory obligations, including recordkeeping, pensions, taxation, and for resolving any employment-related claims or references.
- **Prospective Employees / Recruitment Candidates**: We process the personal data you provide during the recruitment process to assess your suitability for employment, verify your work eligibility, and where applicable, facilitate the issuance of an offer of employment.

4. THE INFORMATION WE COLLECT ABOUT YOU

Depending on your relationship with us, the Bank may collect the following categories of personal data:

- **Identification Data**: Full name, date of birth, gender, nationality, photograph, ID documents
- **Contact Details**: Home address, email address, phone numbers
- **Employment Details**: Position, department, employee ID, job history, promotions, transfers, and exit details
- **Recruitment Information**: CVs/resumes, qualifications, employment history, references, assessment results
- **Background and Educational Information**: Academic credentials, employment history, criminal record (where required)
- **Compensation Data**: Salary, bonuses, benefits, pension, and tax information
- **Sensitive Personal Data**: Health information, religion (if provided), disability status, biometric data (e.g., fingerprints for access control)
- **Family Information**: Spouse and dependents' names, dates of birth, and contact details
- **IT and System Usage Data**: Email usage, access logs, system activity, and device usage logs
- **Legal/Compliance Data**: Disciplinary records, investigations, regulatory filings

5. WHY WE COLLECT YOUR INFORMATION

Your personal data is collected and processed for legitimate business and regulatory purposes, including but not limited to:

- Recruitment, background verification, and eligibility checks
- Onboarding, contract administration, and benefits management
- Profiling on IT systems and provisioning of work tools
- Compliance with employment, tax, and pension laws
- Legal or disciplinary investigations
- Business operations and HR administration
- Security, fraud detection, and policy enforcement
- Internal analytics to improve employee experience
- Any other lawful purpose permitted by applicable regulations

6. WHY WE SHARE PERSONAL DATA

Your data may be shared internally (on a need-to-know basis) and with third parties such as:

- Pension administrators and HMOs
- Payroll service providers and banks
- Regulators (e.g., CBN, NDPC, PENCOM, FIRS)
- Law enforcement agencies (when required)
- External auditors, consultants, or legal representatives
- Background verification and screening providers

All third-party processors are bound by confidentiality and data protection agreements in line with the NDPA.

7. WORKPLACE MONITORING

We maintain strong technical and organizational security controls to protect your personal data from unauthorized access, alteration, or loss. These include:

- Encryption and secure data storage
- Role-based access to systems
- Regular audits and compliance checks
- Network and endpoint monitoring
- Monitoring of email, system use, and physical premises (via CCTV and access controls) is conducted to ensure policy compliance, prevent misconduct, and safeguard Bank assets.

8. HOW LONG WE HOLD YOUR INFORMATION

We will only retain your personal data for as long as is reasonably necessary to fulfill the purposes for which it was collected, including to satisfy any legal, regulatory, tax, accounting, or reporting requirements.

- **Employees and Outsourced Staff:** Personal data will be retained throughout the period of your employment/engagement with the Bank and thereafter for a period necessary to comply with legal obligations, resolve disputes, and enforce contractual rights.
- **Former Employees:** Personal data will be retained for the period required by applicable laws and regulations after the termination of employment. This is to ensure compliance with legal, regulatory, and contractual obligations, as well as to manage potential legal claims.
- **Prospective Employees / Recruitment Candidates:** We retain the personal data of unsuccessful candidates for up to **6 months** after the conclusion of the recruitment process, unless a longer retention period is permitted by you, required by law or necessary for the establishment, exercise, or defense of legal claims. After this period, the data will be securely deleted or anonymized. If you are successful and accept an offer of employment with the Bank, the personal data collected during the recruitment process will form part of your employee records and will be retained in line with our employee data retention practices.

After the expiration of the relevant retention periods, personal data will either be securely deleted, anonymized, or archived in compliance with applicable laws and the Bank's internal policies.

9. YOUR RIGHTS

You have rights conferred on as a Data Subject (in respect of your personal data with the Bank) by applicable regulations and laws such as the Nigeria Data Protection Act (2023).

You are entitled to:

1. Request for and access personal data collected and stored by Fidelity Bank.
2. Withdraw consent at any time.
3. Object to automated decision making.
4. Request rectification and modification of data kept by Fidelity Bank.
5. Request for deletion of data.
6. Be informed of and entitled to provide consent prior to the processing of data for purposes other than that for which the personal data is collected.
7. Request the movement of data by Fidelity Bank to a Third Party; this is the right to the portability of data.
8. Request that Fidelity Bank restricts the processing of such information.
9. Seek redress from the Nigeria Data Protection Commission.

Where Fidelity Bank will be unable to act on the request of a Data Subject exercising his/her rights, the Bank shall inform such Data Subject 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 the Nigeria Data Protection Commission (NDPC).

Information provided to Data Subjects shall be free of charge. However, Fidelity Bank may charge administrative costs for providing information or taking actions requested by a Data Subject for manifestly unfounded, repetitive, or excessive requests by such the Data Subject.

10. YOUR OBLIGATIONS

As an employee (current or former), candidate, or outsourced staff, you are obligated to:

- Maintain the confidentiality of non-public data accessed in the course of your role
- Refrain from disclosing personal data to unauthorized persons
- Only access or process personal data for legitimate work-related purposes
- Report data breaches or suspicious activity immediately to the DPO
- Forward all Data Subject Access Requests to the Data Protection Officer
- Adhere to all applicable data protection policies and procedures

11. DATA BREACH MANAGEMENT PROCEDURE

All Employees are required to read and understand the Bank's Data Breach Management Procedure, which can be accessed on the Data Protection and Privacy SharePoint portal. Any breach of the Data Breach Management Procedure may attract disciplinary procedures, up to termination of employment or dismissal.

All employees must inform the Data Protection Officer (DPO) immediately about cases of suspected or confirmed breach in line with the Data Breach Management Procedure.

12. CHANGES TO THE NOTICE

This policy shall be reviewed every two years or as needed, based on changes in the law, guidance from the NDPC, or changes in the bank's data processing activities.

13. CONTACT FOR ANY QUERIES

Fidelity Bank has appointed a DPO responsible for overseeing Fidelity Bank's data protection strategy and its implementation to ensure compliance with Nigeria Data Protection Regulation requirements. The DPO should be contacted if you have any queries or clarifications regarding the operation of the Fidelity Bank Data Protection and Privacy Policy or this Notice. The contact details are set out below:

- Data Protection Officer: **Audifax Onuoha**
- Location: **Compliance Group, Fidelity Head Office**

- Phone: **07062570101**
- Email: dataprotection&privacy@fidelitybank.ng