DATA PROTECTION/PRIVACY POLICY

Version 1.5

Date Created	19/09/2018
Document Author	Data Protection Officer
Document Owner	Fidelity Bank
Date Reviewed	30/05/2024
Document Classification	Public
Retention Period	1 Year

Document Control Sheet

Distribution List

Name	Version	Date
Public	Version 1.0	6th June 2019
Public	Version 1.1	22nd May 2020
Public	Version1.2	10th August 2021
Public	Version1.3	1st August 2022
Public	Version 1.4	1st August 2023
Public	Version 1.5	30th May 2024

Change Control

The contents of this document are subject to change control

Document Review

This document is subject to continuous changes. In case there are no changes, then an annual review shall be performed

1. Introduction

Fidelity Bank Plc is a bank licensed in Nigeria by the Central Bank ofNigeria. We provide banking services to a wide variety of customer's 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.

Customers and potential customers can access our services through these channels including our website www.fidelitybank.ng.

By accessing the Bank's services through account opening at the branch and or e-channels and or subscribing to any of our various products such as online banking, instant banking, ATM card services, customers provide certain personal identifiable information.

This document details the policies of the Bank guiding the collection, use, storage, transmission, destruction and disclosure of personally identifiable information.

This policy document is available on our website at www.fidelitybank.ng and our branches. Please read it thoroughly before accessing our service.

By opening an account or accessing or subscribing to any of the Bank's services, you give consent to the processing of your personal data in accordance with this policy.

Unless otherwise defined in this Privacy Policy, terms used in this Privacy Policy have the same meanings as in our Terms and Conditions on www.fidelitybank.ng.

Please read this privacy policy carefully as it will help you make informed decisions about sharing your personal information with us.

1.1 Glossary

"Consent" of the Data Subject 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.

"Data" means characters, symbols and binary on which operations are performed by a computer, which may be stored or transmitted in the form of electronic signals, stored in any format or any device.

"Data Protection Officer" or "DPO" means the person appointed as such under the Data Protection Laws and in accordance with its requirements. A DPO is responsible for advising Fidelity Bank (including its employee) on their responsibilities under the Data Protection Laws, for monitoring compliance with Data Protection Law.

"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.

"NDPR" means the Nigeria Data Protection Regulation, 2019.
"NDPA" means the Nigeria Data Protection Act, 2023.

"Our Services" means the banking services provided by the Bank to the customer, which include but not limited to Online/Mobile banking, Instant banking.

"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.

"Personal Identifiable Information (PII)" means information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in a context.

"PCI DSS" means Payment Card Industry Data Security Standards.

"Processing" means any operation or set of operations, which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

2. Information Collection and Use

We collect several different types of information for various purposes to provide and improve our services to you.

Our data collection points include but not limited to our branches, Head Office location, Automated Teller Machines (ATMs), Mobile Application, Websites. We may also collect your information at events hosted/organized by/for the Bank regardless of if such event is a physical or virtual event.

2.1 Types of Data Collected

2.1.1 Personal Data

While using our services, we may ask you to provide us with certain personally identifiable information that can be used to contact or identify you ("Personal Data"). Personally, identifiable information may include, but is not limited to:

i. Name and Contact Data: We collect your first, middle and last name, email address, bank verification number, postal address, phone number, signature, date of birth, an identification document such as a copy of driver's license, international passport, national identity card, and other similar contact data.

We might also collect personally identifiable information of third parties like your next of kin & guarantor (Note: Please seek the consent of these third parties before providing their information) for several purposes with the goal of granting you access to our services. Such purposes include but are not limited to account opening & obtainment of credit facilities.

ii. Credentials: when you subscribe to any of our products, particularly our e-channels products (Online/Mobile Banking, Instant Banking, Mvisa, Ivy Chatbox) you may be required to provide a User ID, a password, details from a token response device, password hints and similar security information used for authentication and account access. You may also be required or opt to use biometric identification to access your account and authenticate transactions. While this information is required to ensure that you carry out transactions securely, appropriate security measures have been implemented to protect these data including encryption and storage in a secured environment, if required.

iii. Payment Data: If you subscribe to our ATM card products, we will issue you ATM cards each with unique numbers called Personal Access Number (PAN), Personal Identity Number (PIN), and Card Verification Number. You are required to keep your card and these security numbers from access by another person. For certain payment cards, a default PIN may be provided by us. In such circumstances, you are required to change the default PIN to a new PIN to enable activation and/or use of the card. When you carry out transactions or enrollment related to card services or online services, these card security numbers or any of them may be required for authentication.

We collect data necessary to process your payment if you make payment/transfers, such as your card number and the security code associated with your payment card. All payment data are processed, transmitted, and stored securely in line with PCI DSS requirements.

iv. Usage Data: We may also collect information that your browser sends whenever you access our online services and or when you access the services by or through a mobile device ("Usage Data").

This Usage Data may include information such as your computer's Internet Protocol address (e.g. IP address), browser type, browser version, the pages of our Service that you visit, the time and date of your visit, the time spent on those pages, unique device identifiers and other diagnostic data.

When you access services by or through a mobile device, this Usage Data may include the following:

- Geo-Location information: We may request access or permission to and track location-based information from your mobile device, either continuously or while you are using our mobile application, to provide location-based services. If you wish to change our access or permissions, you may do so in your device's settings.
- Mobile Device Access: We may request access or permission to certain features from your mobile device, including your mobile device's camera, calendar, Bluetooth, contacts, storage and other features. If you wish to change our access or permissions, you may do so in your device's setting.
- Mobile Device Data: We may automatically collect device information (such as your mobile device ID, model and Manufacturer), operating system, version information, IP address and diagnostic data.
- Tracking & Cookies Data: We use cookies and similar tracking technologies to track the activity on our Service.

Cookies are files with small amount of data which may include an anonymous unique identifier. Cookies are sent to your browser from a website and stored on your device. Tracking technologies also used are beacons, tags, and scripts to collect and track information and to improve and analyze our Service.
You can instruct your browser to refuse all cookies or to indicate when a cookie is being sent. However, if you do not accept cookies, you may not be able to use some portions of our Service.

v. **Others:** We collect CCTV/Video footage whenever you come into our premises or use our ATMs. We also collect telephone conversations via calls made through any of our contact Centre lines. We also collect facial images through the facial recognition software on our ATMs as stipulated by the Central Bank of Nigeria for fraud prevention.

2.1.2 Sensitive Personal Data

While using our services, we may ask you to provide us with certain sensitive personal data such as Sex (Male/Female), Nationality and Religion, state of origin, date of birth as required by our regulator.

2.2 Use of Analytics to Collect/Monitor/Analyze Data

We may use third-party Service Providers to monitor and analyze the use of our Service.

2.2.1 Google Analytics

Google Analytics is a web analytics service offered by Google that tracks and reports website traffic. Google uses the data collected to track and monitor the use of our Service. This data is shared with other Google services. Google may use the collected data to contextualize and personalize the ads of its own advertising network.

For more information on the privacy policies of Google, please visit the Google Privacy & Terms web page located at Privacy Policy – Privacy & Terms – Google

2.2.2 Addthis

Oracle Corporation operates AddThis.com, a social bookmarking service that can be integrated into a website with the use of a web widget. This is used to share content from our website to social media platforms such as Facebook, Myspace, Google Bookmarks, Pinterest, and Twitter.

AddThis analytics also allow us to track how, where, and by whom our content is being shared. In addition, the analytics show follow activity, related posts performance, visits, and conversions.

You can prevent AddThis from using your information for analytics purposes by opting out. To opt-out of AddThis service, please visit this page: addthis.com/privacy/opt-out/

For more information on what type of information AddThis collects, please visit the Terms of Use page of AddThis addthis.com/privacy/terms-of-service/

We also use other third-party providers like Netcore Platform Script, Facebook and other scripts to collect anonymous information such as the number of visitors to the site, and the most popular pages.

You have the option to accept or reject usage of nonessential cookies when you visit our website. Should you wish to stop the usage of the nonessential cookies, you can delete such cookies associated with our website on your browser.

2.2.3 Links to Other Sites

Our Service may contain links to other sites that are not operated by us. If you click on a third-party link, you will be directed to that third party's site. We strongly advise you to review the Privacy Policy of every site you visit.

We have no control over and assume no responsibility for the content, privacy policies or practices of any third-party sites or services.

2.3 Use of Data

The purpose of collecting personally identifiable information is to enable us to provide you with the banking services you have subscribed to and ensure that you are able to carry out transactions without hitches.

The usage of data may be extended beyond the above whenever necessary for the purposes of meeting legal, regulatory, contractual obligations, and other legitimate business interests.

Specifically, the uses the Bank could put your data into include but not limited to:

i. To provide and maintain our services

ii. To notify you about changes to our service

iii. To allow you to participate in interactive features of our service when you choose to do so

iv. To provide customer care and support

v. To provide you access to loyalty benefits.

vi. To provide information to Credit Agencies

vii. To comply with Laws and Regulations

viii. To comply with our Internal Policies

ix. To provide analysis or valuable information so that we can improve our services.

x. To monitor the usage of our Service

xi. Monitor our conversation with you when we speak on the telephone (for example, to check your instructions to us, to analyze, to assess and improve customer service; for training and quality assurance purposes; for verification, fraud analysis and prevention purposes

xii. Recover any debts that you may owe the Bank.

xiii. To detect, prevent and address technical issues.

xiv. To facilitate account opening

xv. To send you marketing and promotional communications for business purposes.

xvi. To deliver targeted advertising to you for our Business Purposes and/or with your consent. We may use your information to develop and display content and advertising (and work with third parties who do so) tailored to your interests and or location and to measure its effectiveness.

3. Basis for Lawful Processing

The Bank processes data in accordance with the Nigeria Data Protection Regulation and the Nigeria Data Protection Act, 2023. The Bank relies on the basis for lawful processing stated below.

i. The data subject has given and not withdrawn his consent for the specific purpose or purposes for which it will be processed;

ii. 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,

- For compliance with a legal obligation to which the data controller or data processor is subject,

- In order to protect the vital interest of the data subject or another individual,

- For the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller or data processor, or

- For the purposes of the legitimate interests pursued by the data controller or data processor or by a third party to whom the data is disclosed so no such legitimate interests are within the scope of the Nigeria Data Protection Act, 2023.

4. Transfer of Data

The world today is interconnected and so is the provision of banking services. For instance, there could be many counterparties involved for a card transaction to be successfully completed. These include the personalization companies, the switching companies, processors, acquirers, merchants, and the card schemes. Certain personal data will traverse these parties in the normal course of carrying out transactions.

Save as related to the provision of banking services and meeting legal, regulatory, contractual, and other uses tangential or incidental to these, Fidelity will not share your personal data with a third party. Where it becomes necessary to do so, adequate security measures will be taken to protect the data from access by recipients other than those for which it is intended. All data we collect will reside in Fidelity's computer systems in Nigeria. Where cloud services are used, adequate governance measures that apply to such cloud services will be complied with.

Fidelity Bank Plc will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this Privacy Policy. No transfer of your Personal Data will take place to an organization or a country unless there are adequate controls in place including the security of your data and other personal information.

4.1 Transfer of Personal Data to a Foreign Country

Where Personal Data is to be transferred to a country outside Nigeria, the Bank shall put adequate measures in place to ensure the security of such Personal Data. In particular, the Bank shall, among other things, conduct a detailed assessment of whether the said country is on the National Information Technology Development Agency's (NITDA's) Whitelist of Countries with adequate data protection laws.

Transfer of Personal Data out of Nigeria would be in accordance with the provisions of the Nigeria Data Protection Regulation, 2019 (NDPR) and the Nigeria Data Protection Act, 2023 (NDPA). The Bank will therefore only transfer Personal Data out of Nigeria or process data on one of the following conditions:

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

ii. It is necessary for the performance of a contract between the Bank and the Data Subject or implementation of pre-contractual measures taken at the Data Subject's request;

iii. It is necessary to conclude a contract between the Bank and a third party in the interest of the Data Subject;

iv. It is necessary for reason of public interest;

v. It is for the establishment, exercise or defense of legal claims;

vi. It 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.

vii. It is necessary for the purposes of the legitimate interests pursued by the Bank or by a third party to whom the data is disclosed.

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 provision 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.

The 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 upon the Data Subject's request.

Where the recipient country is not on the Whitelist and none of the conditions stipulated in this Privacy Policy are met, the Bank will engage with Nigeria Data Protection Commission and the Office of the Honorable Attorney General of the Federation (HAGF) for approval with respect to such transfer.

5. Disclosure of Data

We only share and disclose your information in the following situations:

i. Performance of Contractual Obligations: We may disclose your data to perform and conclude a contract in the interest of the Data Subject. The interest of the Data Subject includes but is not limited to provision of financial services.

ii. Compliance with Laws: We may disclose your information where we are legally required to do so in order to comply with applicable law, governmental requests, a judicial proceeding, court order, or legal process, such as in response to a court order or a subpoena (including in response to public authorities to meet national security or law enforcement requirements).

iii. Vital interests and Legal Rights: We may disclose your information where we believe it is necessary to investigate, prevent, or take action regarding potential violations of our policies, suspected fraud, situations involving potential threats to the safety of any person and illegal activities, or as evidence in litigation in which we are involved.

iv. Vendors, Consultants and Third-party Service Providers: We may share your data with third party vendors, service providers, contractors or agents who perform services for us or on our behalf and require access to such information to do that work, which is necessary to provide the envisaged banking services. Examples include but not limited to: payment processing, data analysis, email delivery, hosting services, customer service and marketing efforts. For the purpose of service improvement, we may allow selected third parties to use tracking technology on the services which will enable them to collect data about how you interact with the services over time. This information may be used to, among other things, analyze and track data, determine the popularity of certain content and better understand online activity. Unless described in this policy, we do not share, sell, rent, or trade any of your information with third parties for their promotional purposes.

v. Business transfers: we may share or transfer your information in connection with, or during negotiations of, any merger, sale of company assets, financing, or acquisition of all or a portion of our business to another company.

With your consent we may disclose your personal information for any other purpose.

6. Security of Data

The security of your data is important to us. We have implemented appropriate technical and organizational security measures designed to protect the security of any personal information we process. However, please also remember that we cannot guarantee that the internet in itself is 100% secure. Although we will do our best to protect your personal information, but transmission of personal information to and from our services is at your own risk. You should only access the services within a secure environment.

7. General Principles for Processing of Personal Data

The Bank is committed to maintaining the principles in the NDPR & NDPA regarding the processing of Personal Data.

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

7.1 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 the 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 NDPR 2019 and the NDPA 2023.

7.2 Data Accuracy

Personal Data must be accurate and kept up to date. In this regard, the Bank shall:

i. 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.

ii. make efforts to keep Personal Data updated where reasonable and applicable; and

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

7.3 Purpose Limitation

The Bank collects Personal Data only for the purposes identified in the

appropriate 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, save where the processing is otherwise allowed by law or within other legal grounds recognized in the NDPR 2019 and the NDPA 2023.

7.4 Data Minimization

The Bank limits Personal Data collection and usage to data that is relevant, adequate, and necessary for carrying out the purpose for which the data is processed. The Bank will evaluate whether and to what extent the processing of personal data is necessary and where the purpose allows, anonymized and/or pseudonymized data must be used.

7.5 Integrity and Confidentiality

i. The 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.

ii. 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.

iii. 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.

iv. 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.

v. 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.

7.6 Personal Data Retention

i. All personal information shall be retained, stored and destroyed

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

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

iii. the contract terms agreed between the Bank and the Data Subject or as long as it is needed for the purpose for which it was obtained; or

iv. whether the transaction or relationship has statutory implication or a required retention period; or

v. whether there is an express request for deletion of Personal Data by the Data Subject, provided that such request will only be treated where there are no legal or regulatory requirements to keep such data, or the Data Subject is not under any investigation which may require the 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

vi. whether the 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 NDPR 2019 and the NDPA 2023, the Bank shall be entitled to retain and process Personal Data for archiving, scientific research, historical research, or statistical purposes for public interest.

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

ii. We will only keep your personal information for as long as it is

necessary for the purposes set out in this Privacy Policy unless a longer retention period is required or permitted by law.

iii. Upon request for account closure, your account will be closed but this closure will not involve deletion of historical records of the account for the reasons already stated. However, except as may be required by law or law enforcement agents and or regulators, further processing of the personal information related to the account will cease from the time of closure.

7.7 Accountability

i. The Bank demonstrates accountability in line with the NDPR and NDPA obligations by monitoring and continuously improving data privacy practices within the Bank.

ii. Any individual or employee who breaches this Privacy 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.

iii. When a potential breach has occurred, the Bank will investigate to determine if an actual breach has occurred and take the necessary actions required to manage and investigate the breach. Such actions include:

- Validating the Personal Data breach.
- Ensuring proper and impartial investigation (including digital forensics if necessary) is initiated, conducted, documented, and concluded.
- Identifying remediation requirements and track resolution.
- Reporting all findings to the top management.
- Coordinating with appropriate authorities as needed.
- Coordinating internal and external communications.
- Ensuring that impacted Data Subjects are properly notified, if necessary.

8 Children's Privacy

The Bank has a children's account called "SWEETA". This account is opened and run by a child's parent or guardian until the child reaches the age of maturity. All personal information pertaining to such account is provided by the parent / guardian. A parent or guardian should therefore read this policy thoroughly to understand how the data provided is handled.

Students of tertiary institution with valid identification, admission letter to a tertiary institution and passport photographs can open the Fidelity Flex Account. Such customers' personal data will be processed as adult's data as long as the individual is above the age of eighteen (18) as contained in the section 65 of the NDPA. Other than as related to the operation of the aforementioned children's account and student's account, the Bank does not enter into banking relationship with minors (persons under the age of 18).

We do not knowingly collect personally identifiable information from anyone under the age of 18 except under the conditions stated above or where the age of the individual cannot be determined. If you are a parent or guardian and you are aware that your children have provided us with Personal Data, please contact us. If we become aware that we have collected Personal Data from children without verification of parental consent, we will take steps to remove that information from our servers.

9 Your Privacy Rights

As data subjects you have certain rights under applicable data protection laws such as the NDPR & NDPA for Nigeria and the GDPR for European countries. These may include the right

i. to request access and obtain a copy of your personal information.

ii. to request rectification or erasure.

iii. to restrict the processing of your personal information and if applicable.

iv. to data portability.

v. In certain circumstances as stated in section 2.8 of the Nigeria Data Protection Regulation, you may also object to the processing of your personal information. To make such a request, please use the contact details provided below. We will consider and act upon any request in accordance with applicable data protection laws.

vi. to lodge a complaint with the Nigeria Data Protection Commission

If we are relying on your consent to process your personal information, you have the right to withdraw your consent at any time. Please note however, that this will not affect the lawfulness of the processing before its withdrawal.

If you are resident in the European Economic Area and you believe we are unlawfully processing your personal information, you also have the right to complain to your local data protection supervisory authority. You can find their contact details here: https://edpb.europa.eu/about-edpb/board/members_en

10 Account Information

If you would at any time like to review or change the information in your account or terminate your account, you can contact us using the contact information provided.

Cookies and Similar technologies: Most web browsers are set to accept cookies by default. If you prefer, you can usually choose to set your browser to remove cookies and to reject cookies. If you choose to remove cookies or reject cookies, this could affect certain features of our services to you. To opt-out of interest-based advertising by advertisers on our services visit http://www.aboutads.info/choices/

Opting out of email marketing: You can unsubscribe from our marketing email list at any time by clicking on the unsubscribe link in the emails that we send or by contacting us using the details provided below. You will then be removed from the marketing email list - however, we will still need to send you service-related emails that are necessary for the administration and use of your account. To otherwise opt-out, you may:

i. Note your preferences when you register an account with the site

ii. Access your account settings and update preferences.

iii. Contact us using the contact information provided

11 Automated individual decision-making or profiling

We do not use any automated processing systems for coming to specific decisions – including profiling.

12 Training

The 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 Privacy Policy, the NDPR and the Nigeria Data Protection Act (2023) with regard to the protection of Personal Data. On an annual basis, the Bank shall develop a capacity building plan for its employees on data privacy and protection in line with the NDPR and the Nigeria Data Protection Act (2023).

13 Data Protection Officer

The Bank shall appoint a Data Protection Officer (DPO) responsible for overseeing the Bank's data protection strategy and its implementation to ensure compliance with the NDPR and the Nigeria Data Protection Act (2023) requirements. The DPO shall be a knowledgeable person on data privacy and protection principles and shall be familiar with the provisions of the NDPR and the Nigeria Data Protection Act (2023).

The main tasks of the DPO include:

i. administering data protection policies and practices of the Bank;

ii. monitoring compliance with the NDPR 2019, the NDPA 2023 and other data protection laws, data protection policies, awareness-raising, training, and audits;

iii. advice the business, management, employees and third parties who carry on processing activities of their obligations under the NDPR 2019 and the NDPA (2023);

iv. acts as a contact point for the Bank;

v. monitor and update the implementation of the data protection policies and practices of the Bank and ensure compliance amongst all employees of the Bank;

vi. ensure that the Bank undertakes a Data Protection Impact Assessment and curb potential risk in the Bank's data processing operations; and

vii. maintain a database of all the Bank's personal data collection and

processing activities.

14 Data Protection Audit

The Bank shall conduct an annual data protection audit through a licensed Data Protection Compliance Organization (DPCO) to verify the Bank's compliance with the provisions of the NDPR, the NDPA (2023) and other applicable data protection laws.

The audit report will be certified and filed by the DPCO to Nigeria Data Protection Commission as required under the NDPR and the NDPA (2023).

15 Changes to This Privacy Policy

We may update our Privacy Policy from time to time. We will notify you of any changes by posting the new Privacy Policy on this page and making it available at our branches.

You are advised to review this Privacy Policy periodically for any changes. Changes to this Privacy Policy are effective as of the date it is made public.

16 Contact Us

If you have any further questions or comments about us or our policies, email us at true.serve@fidelitybank.ng or by post to:

Fidelity Bank Plc
2 Kofo Abayomi Street
Victoria Island Lagos
Nigeria
Phone: 070034335489

If you have any inquiries or grievances about this policy, or how Fidelity Bank (or any of the bank's third parties) handles or have handled your personal data, or how your complaint has been handled, you have the right to lodge a complaint directly with the Fidelity Bank Data Protection Officer. You may contact our Data Protection Officer (DPO) by email at DataProtection&Privacy@fidelitybank.ng or by post to:

Data Protection Officer
Fidelity Bank Plc
2 Kofo Abayomi Street
Victoria Island Lagos
Nigeria

However, if you are aggrieved by the decision, action, or inaction of the bank or any of its third-party processor you may lodge a complaint with the Commission via email at dpo@ndpc.gov.ng or by post to:

Data Privacy Service Unit
Nigeria Data Protection Commission
No.12 Clement Isong Street,
Asokoro,
Abuja,
Nigeria