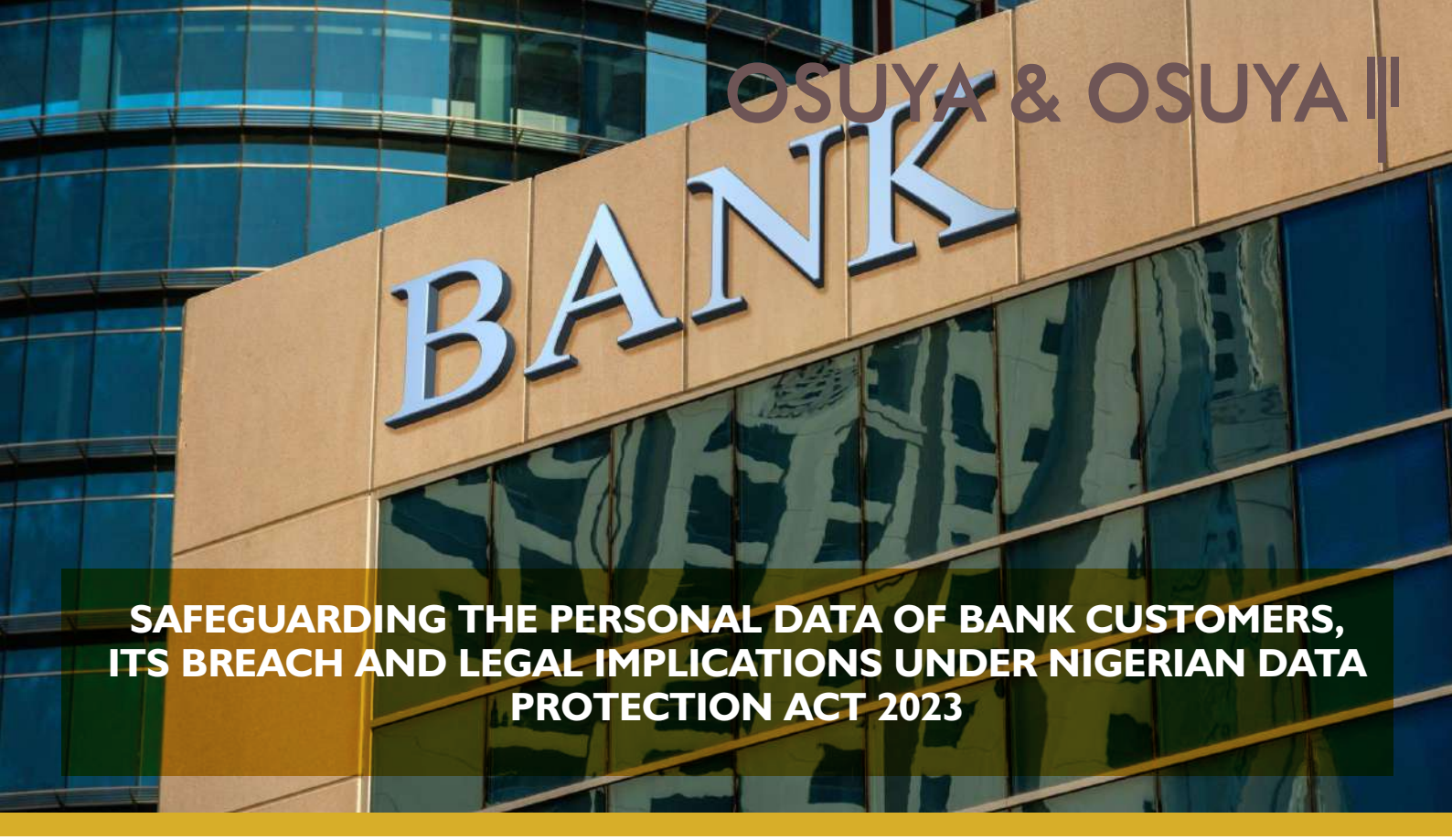


OSUYA & OSUYA

SAFEGUARDING THE PERSONAL DATA OF BANK CUSTOMERS, ITS BREACH AND LEGAL IMPLICATIONS UNDER NIGERIAN DATA PROTECTION ACT 2023

Key Contacts

PETER NDUBUISI AKPU
Designation: Associate
Area of Specialization: Fintech law, Data privacy and white-collar crimes

CHUKWUKA OGOCHUKWU FAITH
Designation: Associate
Area of Specialization: Litigation, property and international law

INTRODUCTION

According to the Nigerian Data Protection Act 2023 ("the Act"), Data can be said to be characters, symbols, or 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, while "Personal Data" (PD) means any information relating to an identified or identifiable natural person. According to the Act, a Data Subject (DS) is an identifiable natural person 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.

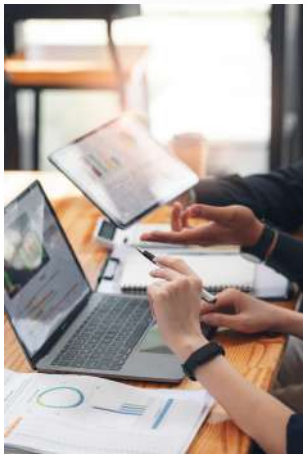
The acknowledgment of the need for data protection in Nigeria was prompted by advancements in technology and the rise of the digital economy. Legislative activities also influenced this recognition in other jurisdictions. Despite these regulatory efforts, data protection in Nigeria still faces challenges. Data protection in Nigeria has had a turbulent past which is characterized by inadequate record-

keeping, lack of judicial interest, and political disputes. According to some experts, the Computer Security and Critical Information Infrastructure Protection Bill[1] marked the initial significant effort to regulate data protection in the country. While the 1999 Constitution of the Federal Republic of Nigeria[2], guarantees and protects the privacy of citizens, their homes, correspondence, telephone conversation, and telegraphic communications, it lacks the explicit provisions present in the constitutional documents of other countries or organizations like Argentina, and the European Union. On the other hand, the Nigerian constitution does not explicitly mention data protection or provide for its explicit protection. However, there has been a recent development in Nigeria where the Court of Appeal, in its first appellate resolution on the subject, has offered some guidance by stating that data protection is guaranteed by, and subsumed under Section 37, of the Constitution which provides for right to privacy[3].

Data protection has become a significant concern in today's digital age, particularly in the banking sector, where handling personal and financial information is inevitable. As banks increasingly rely on technology to provide efficient and convenient services, ensuring robust data protection measures is essential to maintaining trust, protecting customer privacy, and defending against cyber threats. Data has become a valuable asset in an increasingly digital economy, and protecting it has become paramount. Nowhere is this more critical than in the banking sector, where sensitive financial information is entrusted to financial institutions by their customers.

In Nigeria's financial sector, the Banking and Other Financial Institutions Act regulates banking and other financial institutions and matters connected to them. The Central Bank of Nigeria ('CBN'), through the Central Bank of Nigeria Act[4] also regulates the banking sector. The BOFIA and CBN Act do not make specific provisions for data protection in the finance sector. However, specific guidelines issued by the CBN, such as the Consumer Protection Framework ('the Framework') and the draft Consumer Protection Guidelines of Disclosure and Transparency, make some provisions for data protection and privacy in the financial sector.The Nigeria Data Protection Regulation (NDPR), although considered as a subsidiary legislation, is the extant data oide in Nigeria and mainly makes provisions for the protection of the personal data of individuals as opposed to that of corporate and legal entities.

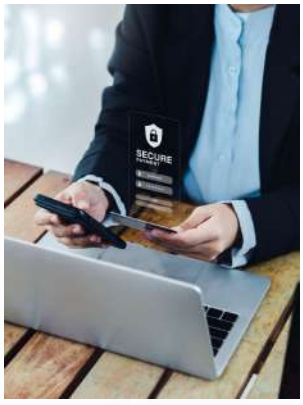
1 2005
2 S.37
3 Digital Rights Lawyers Initiative (DRLI) v National Identity Management Commission (NIMC), CA/IB/291/2020.
4 CBN Act 2007



This article will delve into the importance of data protection in the banking sector, explore its challenges, and highlight the measures to be taken, to ensure the security and privacy of customers' financial data with relative cognizance of the Nigeria Data Protection Regulation. (NDPR) 2019, Nigeria Data Protection Act 2023 and its provisions on data protection for the personal data of individuals.

MEANING OF DATA PROTECTION UNDER THE BANKING AND FINANCIAL SECTOR

In Nigeria, while various legislation contains provisions for data protection, the most comprehensive regulatory instrument is the Nigeria Data Protection Act (the "Act") which has repealed the Nigeria Data protection regulation 2019 issued by the National Information and Technology Development Agency (NITDA) under the authority of NITDA Act. This Act controls how the PD of DS is to be handled and protected to avoid data breaches. Data protection and data security of the PD of bank customers are distinct yet interconnected concepts. Data protection pertains to safeguarding personal information from unauthorized access use or disclosure, ensuring protection of personal information from authorized access, use or disclosure, and ensuring it is used solely for intended banking purposes and not shared without explicit consent. On the other hand, data security focuses on protecting information from unauthorized access or theft by implementing measures like encryption, firewalls, and access control. Therefore, data protection and security are closely linked, as ensuring privacy will necessitate robust security measures. Both are essential for safeguarding personal information, preventing misuse, and addressing concerns of individuals, businesses, and governments in an increasingly digital world where data collection, processing and sharing are prevalent.



SAFEGUARDING THE PERSONAL DATA OF CUSTOMERS IN THE BANKING SECTOR

Protecting customers' data is essential for building and maintaining trust and confidence in the banking industry and constitutes a legal and ethical obligation, according to the Act. Banks, as data controllers of Millions of their customers' PD, handle various types of personal information, including financial records, transaction details, identification documents, contact information etc. and

unauthorized access, misuse, or mishandling of this data can lead to severe consequences, such as financial loss, identity theft, reputational damage, and legal liabilities. The Cybercrimes (Prohibition and Prevention etc.,), Act 2015 establishes an all-encompassing legal, regulatory, and institutional framework in Nigeria to prevent, detect, prosecute, and impose penalties for cyber offenses. Hence the banks must ensure that their customers' data are duly protected and that their rights to the protection and safeguard of their personal information are protected, as catered for under the Nigerian Data Protection Act 2023. By the provision of section 39[5] of the Act, banks and other financial institutions should employ suitable technical and organizational measures to guarantee the security, integrity, and confidentiality of personal data in their possession or control. These measures should include protection against accidental or unlawful destruction, loss, misuse, alteration, unauthorized disclosure, or access. According to the Act[6], bank customers need to understand that in the event of a personal data breach that poses a high risk, to guarantee the protection of their rights, the bank must promptly inform the customers using clear and straightforward language. Thus, communication should include guidance and actions the customer can take to effectively minimize any potential negative consequences resulting from the breach. Where directly contacting the customer (s) is impractical due to the expenses, or feasibility, the bank may choose to make a public announcement through widely accessible media sources to ensure that the customers are duly informed[7]

IMPORTANCE OF DATA PROTECTION IN THE BANKING SECTOR

There are several compelling reasons why data protection is highly significant in the financial sector. Data protection is of utmost importance in the banking sector due to the nature of the information being handled. Banks store and process vast amounts of personal and financial data, including account details, transaction records, and credit history. Such information, if compromised, could lead to severe consequences, including financial loss, identity theft, and reputation damage for both customers and banks. **Part one, Section 1.1 of the Nigeria Data Protection Regulation ---Objectives of the regulation,** establishes various objectives of the regulation and identifies the significance of Data protection in the Banking sector, which include the following;

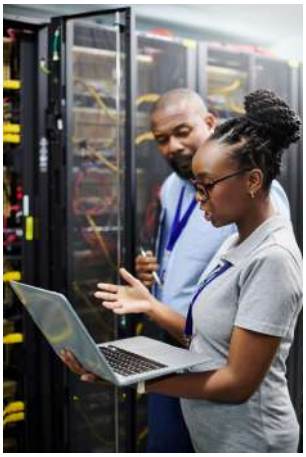
a) to safeguard the rights of natural persons to data privacy;

5 Nigerian Data Protection Act, 2023
6 (3)
7 file:///C:/Users/USER/Downloads/Assessing-data-protection-in-NigeriaFinal.pdfAccessed 3rd July 2023

b) to foster safe conduct for transactions involving the exchange of Personal Data;
c) to prevent manipulation of Personal Data; and
d) to ensure that Nigerian businesses remain competitive in international trade through the safeguards afforded by a just, equitable, legal, and regulatory framework on data protection and which is in tune with international best practices

1. Protecting Customer Privacy:

Banks hold vast amounts of personal and financial data, making them attractive targets for cybercriminals. Safeguarding customer privacy is a top priority, and banks employ strong security measures such as encryption, access controls, and secure data storage to prevent unauthorized access or data breaches. Regular audits and risk assessments are conducted to identify vulnerabilities and ensure compliance with privacy regulations.



2. Strengthening Cybersecurity in the Exchange of Personal Data:

With the rise of sophisticated cyber threats, banks invest heavily in cybersecurity to protect against data breaches, fraud, and identity theft. Multi-factor authentication, firewalls, intrusion detection systems, and continuous monitoring are essential for detecting and mitigating cyber threats. Regular security training for employees helps create a culture of awareness and vigilance.

3. Compliance with Regulatory Standards:

The banking sector operates under stringent regulations to protect customer data. Compliance with the General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI DSS) is crucial. These regulations outline data collection, storage, and sharing guidelines, ensuring data protection, transparency, and accountability.

4. **Data Encryption and Anonymization to ensure the competitiveness of Nigeria's Business in International Trade:**

Sensitive customer data, such as account details and transaction history, is often encrypted to prevent unauthorized access. Encryption transforms data into a coded format that can only be deciphered with the appropriate decryption key.

Fundamental Principles of data protection in the banking sector

The banking sector is a highly regulated sector of the Nigerian economy and a data controller of significant importance[8]. Banks engage in the business of accepting money deposits from their customers, transfer, and payment of funds, Internet banking, popularly known as e-banking, money lending services as well as Bill payment, and all these activities require the processing of PD of DS (Customers) like their names, identity cards, and numbers, email address, residential addresses, Account numbers, Banks Verification Number (BVN), etc. The activities of banks in Nigeria are principally regulated by the Banks and Other Financial Institutions Act[9], and the Central Bank of Nigeria is the apex regulator of Banks, including Fintechs and other financial institutions.The Act has captured banks as data Controllers of major significance[10] considering customers' PD volume on their database. Bank customer deposits by top listed banks on the Nigerian Exchange Group (NGX) grew by N32.53 percent to N49 trillion in the nine months of 2022 from N37 trillion in the corresponding period of 2021, data sourced from the Nigerian Exchange Group shows[11]

The top 10 Nigerian Banks published as having the highest number of customers; Access Bank tops the list immediately followed by Eco Bank Plc, Zenith Bank Plc, United Bank for Africa Plc, First Bank of Nigeria Plc, GTCO, Fidelity Bank Plc, FCMB, Union Bank Plc, and Sterling Bank[12]. The Act rightly captured Banking activities and Banks as data controllers of major significance and owes a duty of care to their customers and shall at all times maintain their duty of care and accountability in processing the PD of their customers. Banks should endeavor to process the PD of customers in a fair, lawful and transparent manner, collect their data for a specified, explicit and legitimate purpose and not to be further processed in a way incompatible with these purposes, ensure that the PD is adequate, relevant and limited to the minimum, necessary for the purposes for which the PD was collected and further processed.

Similarly, Banks, in the course of their banking business, should not retain the PD of customers longer than is necessary to achieve the lawful basis for which it is collected or further processed, ensure that the processing of the PD of their customers is accurate, complete, not misleading and where necessary kept up to

8 S.65 Nigeria Data Protection Act
9 BOFIA 2020
10 Section 65 of the Act
11 https://businessday.ng/companies/article/10-banks-with-the-highest-customer-deposits-in-2022/ Accessed 4th July 2023
12 Ibid

date having regard to the purposes for which the PD is collected or further processed; above all ensure that her customers' information is processed in a manner that guarantees utmost security of their PD

including setting up cyber security infrastructure that protects personal data against unauthorized processing, access, loss, destruction, damage or any form of breach[13] Banks, as a major data controller, should ensure that the PD of their customers are processed lawfully.

According to the Act[14] personal data of a data subject is lawfully processed where her customers have given and not withdrawn consent for the specific purpose for which the PD is to be processed or where the processing is necessary for the performance of a legal or contractual obligation imposed on banks either by the Central banks of Nigeria and other regulators or to protect the vital information of her customers or for the performance of a task carried out in the public interest or the exercise of official authority vested in the banks and for the processing of PD on the grounds of legitimate interest. This implies that Banks and her subsidiaries and agents can justify the processing based on legitimate interest. E.g., data processing for the prevention of fraud as imposed by them by the Economic and Financial Crimes Commission (EFCC) or court order, Anti-Money Laundering and Combatting of terrorism financing (AML/CFT) and employee-employer relationships.

It is noteworthy that Banks, in the course of the processing, should have at the back of their mind that legitimate interest will not be a basis for processing personal data in instances where the fundamental rights and freedom of their customers override such interest, where the interest is incompatible with the other lawful bases or where her customers would not have a reasonable expectation that the personal data would be processed in the manner envisaged[15]

DATA PRIVACY IMPACT ASSESSMENT (DPIA) The Act highlights the need for banks to engage the services of Data Protection Officers (DPO) and Data Protection Compliance Organizations (DPCO)[16] for a data protection impact assessment (herein referred to as DPIA) where the processing of PD of her customers appears likely to result in a high risk to the rights and freedoms of data subjects by virtue of its nature[17]. It goes further to mandate the Banks to consult the Commission prior to the processing if the DPIA indicates that the data processing

13 Section 24 Ibid
14 Section 25 Ibid
15 https://oal.law/unveiling-the-nigeria-data-protection-act-2023-an-expert-appraisal-of-key-provisions/#_ftn7> accessed 6th July 2023.
16 Osuya &Osuya Law Firm is a licensed DPCO
17 S. 29 of the Act

would result in a high risk to the rights and freedoms of data subjects. The Act defines a DPIA and also empowers the Commission to issue guidelines and directives on DPIA, including the categories of processing subject to the requirement for a DPIA.

SENSITIVE PD AND THE RIGHTS OF A MINOR OPERATING A BANK ACCOUNT

The Act sets a higher standard of care for sensitive personal data[18]. 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. Generally, a bank or its subsidiaries cannot process sensitive PD except where the data subject has given explicit consent, necessary for vital, legitimate interest but with safeguards, the performance of rights and obligations under employment law, amongst other lawful basis. The Act goes further to state that the Commission may prescribe in rules further categories of PD that may be classified as sensitive PD, further grounds on which such may be processed, and safeguards that may apply.

Similarly, on the rights of a minor[19] operating a bank account or engaging in the banking business, the Act provides that, where a DS is a child or another individual lacking the legal capacity to consent, a data controller shall obtain the consent of a parent[20] or other appropriate legal guardian of the child or other individual, as applicable. Data controllers are also expected to apply appropriate mechanisms in order to verify the age and consent.

CYBER SECURITY AND DATA PROTECTION OF DATA SUBJECTS

Anyone involved in data processing or the control of data shall develop security measures to protect data; such actions include but are not limited to protecting systems from hackers, setting up firewalls, storing data securely with access to specifically authorized individuals, employing data encryption technologies, developing organizational policy for handling Personal Data (and other sensitive or confidential data), protection of emailing systems and continuous capacity building for their staff.

18 S.30 of the Act
19 a person below the age of 18 years
20 S. 30 of the Act

While the Cyber Crimes Act does not strictly function as a data protection legislation, it effectively establishes a comprehensive legal and regulatory framework in Nigeria for addressing cybercrimes. The banking sector is enjoined to promote cyber security and safeguard computer systems, networks, electronic communications, data, intellectual property, and privacy rights. Section 38 of the Cybercrimes Act emphasizes the importance of respecting individuals' right to privacy as enshrined in the 1999 Constitution of the Federal Republic of Nigeria. It mandates that anyone carrying out responsibilities under this section must take suitable measures to preserve the confidentiality of retained, processed, or accessed data in compliance with the law. It is, therefore, crucial for financial institutions to diligently protect customer data to address breaches caused by third parties and ensure that the privacy of data subjects is achieved.

Going by the provision of the Act, laid down procedures have to be followed in dealing with the personal data of customers in the banking sector[21]

i. Personal data must only be collected and processed for specific, legitimate, and lawful purposes as consented to by the data subject. However, there are exceptions where further processing may be allowed for purposes such as archiving, scientific research, historical research, or statistical analysis in the public interest. It is important to note that any individual or organization involved in data processing under these provisions should refrain from transferring personal data to any other entity.

ii. Personal data should be retained only for a reasonable duration during which it is necessary.

iii. Personal data should be safeguarded against all foreseeable risks and breaches, including theft, cyberattacks, viral attacks, unauthorized dissemination, manipulation, and damage caused by rain, fire, or exposure to other natural elements.

iv. It is pertinent for banks and financial institutions in possession of the personal data of a data subject or customers to be obligated to exercise a duty of care towards the respective data subject and shall be accountable for their acts and omissions regarding data processing.

21 Ss. 24, 25, 26 and 27 of the Act

CYBERSECURITY OBLIGATION OF BANKS

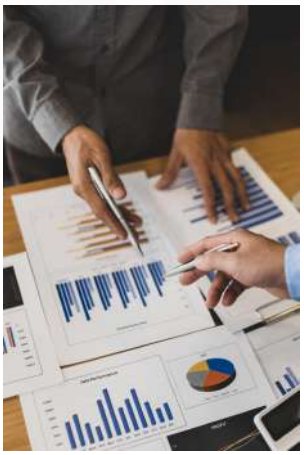
The Act mandates banks and their subsidiaries to implement appropriate technical and organizational measures to ensure the security, integrity, and confidentiality of PD in its care. PD in the control of banks care includes the phone number of customers, Account number of the customers, NIN, BVN, details of ATM Card, money standing in customers' Accounts, etc. It also provides for certain measures that may be implemented to ensure data security, like pseudonymization and de-identification of personal data, encryption, etc.

Another notable addition to the Act is the provision of detailed steps to be taken in case of a data breach of the personal data stored or processed by a data processor. The data processor is mandated to notify the data controller or data processor that engaged it of the nature of the breach and respond to all information requests from the data controller or data processor without delay. Where the breach is likely to result in a risk to the rights of individuals, the data controller is to notify the Commission within[22] of becoming aware. The timeline may be extended where it is reasonably necessary to implement measures required to determine the scope of the breach. The data controller and data processor are also mandated to keep a record of all personal data breaches.

CROSS-BORDER DATA TRANSFERS BY BANKS FOR INTERNATIONAL MONEY TRANSFER (MoneyGram) OR FOREIGN EXCHANGE

This refers to the transfer of personal data to another country or jurisdiction. Generally, a data controller (Banks) or her subsidiaries or agents[23] is not permitted to transfer PD from Nigeria to another country under the Act though subject to limitations. Under the Act, PD can only be transferred from Nigeria to another country if the recipient of the PD is subject to a law, binding corporate rules, contractual clauses, and codes of conduct or certification mechanisms that afford an adequate level of protection with respect to personal data. By the provision[24] of the Act, a level of protection is adequate if it upholds principles that are substantially similar to the conditions for the processing of the personal data provided for in the Act. In addition to the above provisions of the Act, it goes further in Section 44 to enumerate other bases for the transfer of personal data outside Nigeria as contained in the Act. Furthermore, the Act mandates the

22 72 hours
23 Fintech companies like Interswitch
24 S. 43



Commission to create a blacklist of some sort from time to time. It is a list of countries, regions, specific sectors within a country, or standard contractual clauses which the Commission deems as not providing adequate protection for the international transfer of data.

BANKS AS DATA CONTROLLERS AND PROCESSORS OF MAJOR IMPORTANCE.

According to the Act[25], which is also the Interpretation Clause, the Act requires DC and DP of major significance to register with the Commission within six months of the commencement of the Act. The Act defines them as one domiciled, ordinarily resident, or ordinarily operating in Nigeria and processes or intends to process personal data of more than such number of data subjects who are within Nigeria as the Commission may prescribe, or such other class of data of particular value or significance to the economy, society or security of Nigeria as the Commission may designate. The Commission is also empowered to exempt a class of data controllers and processors from registration.

RIGHTS OF A BANK CUSTOMER (DATA SUBJECT) AND CONDITIONS OF CONSENT

The consent of a bank customer may be granted in writing, orally, or through electronic means. In line with the provision of the Act[26], the burden of proof for establishing a data subject's consent is on the DC. It should be noted that the silence or inactivity by the DS shall not constitute consent. The DS can also withdraw his consent at any time. It is important to note that the withdrawal will not affect the lawfulness of prior data processing.

According to the provisions of the Act[27], more elaborate rights of data subjects are provided in contrast to the limited rights of data subjects under the Nigerian Data Protection Regulation 2019. The Act, amongst others, emphasizes that DS (Customers) should have rights to obtaining confirmation of the personal data being processed and details regarding its purpose and retention periods, the right to request rectification or erasure, lodge complaints with the Commission, and request a copy of the personal data in electronic format without undue delay. It also grants data subjects the right to object to the processing of personal data and to not be subjected to a decision based solely on the automated processing of personal data.

25 S. 65
26 S. 27
27 Ss. 35, 36, 37 and 38

SANCTIONS FOR BREACH OF PERSONAL DATA OF BANK CUSTOMERS

The Act[28] provides for sanctions where banks, as data controllers of major importance, fail to imbibe the provisions of the Act in the course of their banking business. Banks are mandated by the act to remedy the violation of the customer's data privacy rights, ordering the bank or her subsidiaries to pay compensation to DS (Customer) who has suffered injury, loss or harm as a result of the violation. The Act also mandates the banks as data controllers to pay a penalty or remedial fee to such a customer for the violation of their data privacy in the course of their business. The remedial fee is classified into "Higher Maximum Amount" and "Standard Maximum Amount", and the penalty and remedial fees that relate to any of the two classifications depend on whether a "data controller" or "data processor", for instance, banks is a data controller of major importance" or "data controllers or data processors of not major importance."

In any event of data privacy violation of the data privacy right of her customers by banks, the Act mandates data Controllers (DC) and Processors of major importance to pay to data subjects(customers) a higher maximum amount which shall be greater than N10,000,000(Ten Million Naira) 0r 2% of its Annual Gross Revenue in the preceding financial year and in the case of data controllers and processors of a not major importance a sum of N2,000,000(Two Million Naira) or 2% of its Annual Gross Revenue in the preceding year.

CONCLUSION:

The Nigerian Data Protection Act contains some novel provisions that regulate the activities of banks in the current Nigerian digital ecosystem, where artificial intelligence is taking over the automation of payment and banking activities. Banks are under obligation to abide by the broader provisions of the Act, to avoid incurring legal liability for data privacy violations.

28 Section 49

OSUYA & OSUYA
LAW FIRM

Abuja

No. 3 Toamasina Street,
Off Adetokunbo Ademola Str,
Wuse II, Abuja
+234 (0) 92910888
+234 (0) 8116168484[whatsapp]
+234 (0)90 22221223

Lagos

No 28 Shakiru Anjorin Street Off. Admiralty Road
Lekki Phase 1 Lagos

Osuya & Osuya Law Firm
Osuya & Osuya Law Firm
Osuya & Osuya Law Firm