# Nigeria - Data Protection in the Financial Sector

**TABLE OF CONTENTS**



**November 2019**

## 1. INTRODUCTION

Other than Section 37 of the Constitution of the Federal Republic of Nigeria 1999 (as amended) ('the Constitution') which provides for the right to privacy of its citizens and a few other pieces of legislation such as the Freedom of Information Act 2011 ('the FoI Act') and the Cybercrimes (Prohibition, Prevention etc.) Act 2015 ('the Cybercrimes Act'), that make reference to data protection in certain sections, there is no all-encompassing legislation that provides for data protection in general or in the financial sector.

That being said, the National Information Technology Development Agency ('NITDA') issued a data protection regulation that now serves as the guide for data protection across the Federation. The Nigeria Data Protection Regulation 2019 ('NDPR') applies to all transactions intended for the processing of personal data, notwithstanding the means by which the data is processed.

The NDPR applies to natural persons residing within Nigeria or outside Nigeria but of Nigerian descent, and does not deny any Nigerian or any natural person the privacy rights they are entitled to under any law, regulation, policy, contract, for the time being in force in Nigeria or in any foreign jurisdiction.

'Personal data' is defined under Section 1.3 of the NDPR as any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is further described as 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. The identifier can be anything from a name, address, photo, email address, bank details, posts on social networking websites, medical information, and other unique identifiers such as a MAC address, IP address, IMEI number, IMSI number, SIM and others.

The NDPR defines 'data controller' as a person who either alone, jointly 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.

In the financial sector, the Banking and other Financial Institutions Act 1991 ('BOFIA') regulates banking and other financial institutions and matters connected to them. The Central Bank of Nigeria ('CBN') through the Central bank of Nigeria Act 2007 ('the CBN Act') also regulates the banking sector. The BOFIA and CBN Act do not make specific provisions for data protection in the finance sector, however, certain guidelines issued by the CBN such as the Consumer Protection Framework ('the Framework'), and recently, the draft Consumer Protection Guidelines of Disclosure and Transparency, make some provision for data protection and privacy in the financial sector.

The NDPR, although considered as subsidiary legislation, is the extant data protection guide in Nigeria and mainly makes provisions for personal data of individuals as opposed to that of corporate and legal entities.

## 1.1. Legislation

**The Constitution**

Section 37 of the Constitution provides for citizens' right to privacy in general and specifies the right to privacy as regards telephone, telegraphic and other forms of correspondence. However, the constitutional provision appears to relate more to privacy than protection.

**The FoI Act**

Section 14 of the FoI Act provides for data privacy by restricting the disclosure of people's personal records in a bid to access public records.

**The Cybercrimes Act**

In 2015, the National Assembly of the Federal Republic of Nigeria enacted the Cybercrimes Act for the purpose of providing an effective umbrella framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes and to protect the national interest. The Cybercrimes Act would also encourage and promote cyber security across the country.

As it relates to organisations, the Cybercrimes Act protects data, access codes and computer systems of individuals and penalises any unlawful acts in relation to that.

**Advanced Fee Fraud and Other Fraud Related Offences Act 2006**

This Act commenced on the 5 June 2006, and while it does not directly provide for data protection, Section 12 provides that entities carrying on electronic telecommunication services should obtain full names, residential address (in the case of an individual), and corporate address (in the case of a corporate body) from their customers/subscribers before providing the said service. This Section implies that the consent of the data subject has been obtained before the service is provided.

**The Framework**

The Framework was issued pursuant to the CBN Act. It prohibits financial institutions from disclosing customers' personal information. It also requires that financial institutions have appropriate data protection measures and staff training programs in place to prevent unauthorised access, alteration, disclosure, accidental loss or destruction of customer data. Furthermore, the Framework requires financial services providers to obtain written consent from consumers before personal data is shared with a third party or used for promotional offers.

The Framework was set up by the CBN to guide the regulation of effective consumer protection practices of financial institutions ('FIs') and ensure that they are adequately protected and treated fairly.

Under the Framework, a consumer refers to a person or an entity that uses, has used, or is a potential user of financial products or services of a FI.

The objectives of the Framework are to:

- protect consumers' assets;
- ensure timely complaints handling and dispute resolution;
- ensure financial services operators put in place effective consumer risk management framework;
- empower consumers to make informed decisions;
- promote professionalism and ethics; and
- outline the rights and responsibilities of consumers.

The Framework makes specific provisions for data protection and privacy in the financial sector and should be studied alongside extant laws like BOFIA and the CBN Act.

**The Risk-Based Cybersecurity Framework And Guidelines For Deposit Money Banks And Payment Service Providers, 2018** ('the CBN Cybersecurity Guidelines')

The CBN Cybersecurity Guidelines were issued by the CBN in October 2018 and represents the minimum requirements to be put in place by all Deposit Money Banks ('DMBs') and Payment Service Providers ('PSPs') in their respective cybersecurity programmes. Among other things, the Cybersecurity Guidelines provide for a Cybersecurity Risk Management System ('the Risk Management System') designed to reduce the incidence of significant adverse impact on an organisation by addressing threats, mitigating exposure, and reducing vulnerability. The Risk Management System covers risk assessment, risk measurement, risk mitigation/risk treatment, and risk monitoring and reporting (Chapter 3 of the CBN Cybersecurity Guidelines). The Cybersecurity Guidelines also

mandate Board and Senior Management of DMBs and PSPs to ensure compliance with all relevant statutes and regulations such as the Cybercrimes Act and all CBN directives to avoid breaches of legal, statutory, regulatory obligations related to cybersecurity and of any security requirements.

The CBN Cybersecurity Guidelines explain the concept of cybersecurity governance and entrusts the board of directors with the power to ensure that the cybersecurity governance of each DMB and PSP not only aligns with corporate and IT governance, but is driven by cyber threat intelligence proactive, resilient, and communicated to all internal and external stakeholders.

The Board is also expected to appoint a Chief Information Security Officer ('CISO') within the DMB or PSP, for the purpose of ensuring that the cybersecurity program of the company is up to date.

DMBs are mandated to set up an Information Security Steering Committee ('ISSC') which will be for the purpose of ensuring that the security policies and processes of the DMBs and PSPs align with the business objectives; evaluating, and sponsoring institution-wide security investments, among others.

In line with the CBN Cybersecurity Guidelines, DMBs and PSPs will be expected to have a cyber crimes strategy and framework as well as a risk management system. The risk management system will involve risk assessment, risk measurement, risk mitigation, risk treatment, and the monitoring and reporting of risks.

All cybersecurity programmes of DMBs and PSPs will be audited by the Internal Audit Committee and the CBN is empowered to ensure compliance. Interestingly, the CBN Cybersecurity Guidelines go further by providing a list of cybersecurity self-assessment tools, templates, and several other benchmarking guidelines which should help DMBs and PSPs to determine whether they meet the compliance criteria or not.

**NDPR**

The NDPR were issued by the NITDA on 25 January 2019. The objectives of the NDPR are to safeguard the rights of natural persons to data privacy, and to foster safe conduct of transactions and prevent manipulation of personal data.

The NDPR applies to all transactions intended for the processing of personal data and to the actual processing of personal data regardless of the means of processing. It also applies to Nigerians living within the country and in the diaspora.

The general rule regarding data protection in Nigeria is that data controllers must obtain the consent of data subjects before they can process their data. The exception to this rule is in the event of 'lawful processing' which includes, where data processing forms part of the performance of contract, where there is a legal obligation to process the data, in order to protect the vital interest of a natural person or, for the purpose of protecting the public interest.

Furthermore, the NDPR provides that organisations must enforce an internal data security program and ensure a valid agreement in the case of third-party data processing.

The NDPR makes provisions for Data Protection Compliance Organisations ('DPCO') that will be licensed by NITDA for the purpose of ensuring compliance of organisations and individuals across the board. The DPCO's are expected to be certified or experienced in data science, information technology, cybersecurity or other related fields, and in order to obtain a license, will typically fall within one of the following categories:

- professional service consultancy firm;
- IT service provider;
- audit firm; or
- law firm.

## 1.2. Supervisory authorities

The relevant regulatory authorities are:

- NITDA
- Economic and Financial Crimes Commission ('EFCC')
- Office of the National Security Adviser ('ONSA')
- CBN

The NITDA is empowered to issue monetary fines against data controllers that are in breach of the privacy rights of data subjects.

The EFCC is not empowered to issue monetary fines as it relates to data protection and cybercrimes.

The ONSA has no specific powers to issue monetary fines.

In relation to the Framework, the CBN is empowered to impose monetary fines as a method of enforcement

enforcement.

# 2. PERSONAL AND FINANCIAL DATA MANAGEMENT

FIs in Nigeria would typically be bound by both the NDPR as well as the financial sector regulations that relate to data protection. The major regulations that would apply to FIs would be the NDPR as it relates to personal information of natural persons as well as the relevant portions of the Framework and the CBN Cybersecurity Guidelines.

## 2.1. Legal basis for processing

A financial institution will be able to lawfully process under the NDPR if they adhere to the provisions within them. As described above, lawful processing could occur if:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is party to or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person; and
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official public mandate vested in the controller.

## 2.2. Privacy notices and policies

Both the NDPR and the Framework contain privacy policies that FIs will be bound by.

The NDPR provides that any instrument for the time being in force or any medium through which personal data is being collected or processed should display a simple and conspicuous privacy policy that the data subjects being targeted can understand. The privacy policy is expected to contain the following alongside other relevant information:

- what constitutes the data subject's consent;
- a description of collectable personal information;
- the purpose of collection of personal data;

- what technical methods are used to collect and store personal information, cookies, web tokens etc.;
- the access (if any) of third parties to personal data and purpose of access;
- any available remedies in the event of a violation of the privacy policy;
- the time frame for the remedy; and
- any limitation clause, as long as it does not avail a data controller who acts in breach of consent.

The Framework provides for the protection of consumer assets and privacy. It states that appropriate measures must be established to ensure that consumer assets and privacy are protected.

It further provides that a consumer's financial and personal information must be protected by FIs at all times and should not be released to a third party without the consent of the consumer, except as required by law.

Under the Framework, the following information are considered to be confidential and must be protected at all times:

- contact details;
- account number and balance;
- statement of accounts; and
- any other information known to the financial institution.

Furthermore, in its data privacy provisions, the Framework states that the personal information of customers (including those with closed accounts) must be strictly confidential. The FIs have a duty of care to safeguard the data of their customers and must not reveal any information to third parties, except under the following circumstances:

- with the express permission of the customer;
- as required by the CBN and other regulatory bodies;
- where there is a court order; or
- in pursuance of public duty/interest;

Appropriate data protection measures and staff training programs shall be put in place to prevent unauthorised access, alteration, disclosure, accidental loss or destruction of customer data.

Note that under the Framework, and as with the NDPR, the consent of consumers must be obtained in writing before their data is shared with third parties (including subsidiaries and associated companies).

3d companies).

FIs are also expected to obtain the consent of customers in writing before using their information for future promotional offers via email, SMS, phone calls etc. and consumers that participate in sales promotions must be notified in the event that they are required to be used for any publicity or advertisement by the financial institution.

## 2.3. Data security and risk management

As regards general data security, the NDPR provides that anyone involved in data processing or the control of data must develop security measures to protect data including:

- measures to protect systems from hackers;
- setting up firewalls;
- storing data securely with access to specific authorised individuals;
- employing data encryption technologies;
- developing organisational policy for handling personal data (and other sensitive or confidential data); and
- protection of emailing systems and continuous capacity building for staff.

The CBN Cybersecurity Guidelines, provides for a Risk Management System to reduce any incidences that could negatively affect an organisation. The risk management system would address threats, mitigate exposure, and reduce vulnerability and all DMBs and PSPs must incorporate cyber risk management with their institution-wide risk management framework and governance requirements to ensure consistent risk management across the institution.

The risk management programme must be based on an understanding of threats, vulnerabilities, risk profile and level of risk tolerance of the organisation. The process is also expected to be flexible enough to change as the risks change.

According to the CBN Cybersecurity Guidelines, the Risk Management System above should cover four basic activities:

- risk assessment;
- risk measurement;
- risk mitigation/risk treatment; and
- risk monitoring and reporting

In addition, cyber risk assessments should be updated regularly and address changes and technological innovation, products, etc. before deployment, to ensure that risk is accurately assessed.

Risk treatment options should then be selected based on the risk assessment.

### 2.4. Data retention/record keeping

In relation to personal data, the NDPR provides that a data subject has the right to request for the deletion of their data and the data controller must delete the said data on one or more of the following grounds:

- the personal data are no longer necessary in relation to the purposes for which they were collected or processed;
- the data subject withdraws consent on which the processing is based;
- the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
- the personal data have been unlawfully processed; and
- the personal data has to be erased for compliance with a legal obligation in Nigeria.

The NDPR requires that a data controller will not retain personal information that is no longer necessary for processing.

## 3. FINANCIAL REPORTING AND MONEY LAUNDERING

In relation to money laundering, the Money Laundering (Prohibition) Act of 2011 and the Terrorism Prevention (Amendment) Act, 2013 are the relevant legislation that would apply.

## 4. BANKING SECRECY AND CONFIDENTIALITY

While there is no legislation in place that provides for banking secrecy and confidentiality, the old English case of *Tournier v National Provincial and Union Bank of England* [1924] 1 KB 461 prescribed the scope of banker-customer secrecy and confidentiality.

In this case, the defendant bank shared one of the plaintiff's confidential information to his employer, after which the employer refused to renew the contract of employment. The Court held that a customer has the right to have his affairs kept confidential, and further held that the duty of secrecy would extend beyond the state of the customer's account, and cover any information generally derived as a result of the account.

The exceptions to this duty are:

- where disclosure is made mandatory by law;
- where disclosure is in the interest of the public;
- where disclosure is in the interest of the bank; and
- where the customer consents to the said disclosure.

## 5. INSURANCE

There are no sectoral regulations specific to data collection and processing in the insurance industry but the Nigeria Deposit Insurance Corporation Act, 2006 regulates insurance practices in Nigeria, for the purpose of insuring all deposit liabilities of licensed banks and other financial institutions operating in Nigeria.

It also provides assistance in the interest of depositors in case of financial difficulties; guaranteeing payments to depositors in case of imminent suspension of payments by insured banks and other financial institutions and assisting the authorities in creation and implementation of banking policies.

## 6. PAYMENT SERVICES

The Cybersecurity Framework would relate to PSPs.

## 7. DATA TRANSFERS AND OUTSOURCING

As regards the transfer of data, the NDPR provides for processing of a data subject's personal information by a third party as well as transfer of data to a foreign country.

As regards third-party processing, a written contract must be put in place between the third party and the data controller before transferring any data for processing. Accordingly, any person engaging a third party to process the data obtained from data subjects must follow these practices.

In relation to the transfer of data to a foreign country, the Honourable Attorney General of the Federation ('AGF') has supervisory authority over said transfer. Accordingly, data can only be transferred to a foreign country on the following grounds:

- where the NITDA has decided that the foreign country, territory or one or more specified sectors within that foreign country, or the international organisation in question ensures an adequate level of protection;
- where the AGF has taken into consideration the legal system of the foreign country particularly in the areas of rule of law, respect for human rights and fundamental freedom, relevant legislation, both general and sectoral, including public security, defence, national security, criminal law, and the access of public authorities to personal data;
- where the foreign country implements a data protection regulation, including rules for the onward transfer of personal data to another foreign country or international organisation which are complied with in that country or international organisation;
- where there is an effective functioning of one or more independent supervisory authorities in the foreign country or to which an international organisation is subject, in order to ensure compliance with data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the relevant authorities Nigeria; and/or
- consideration of the international commitments or international organisations that the foreign country has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in relation to the protection of personal data has been taken.

In the absence of any decision by the NITDA or AGF to the contrary, transfer of data to a foreign country can take place if:

- the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of the same;
- the transfer is necessary for the performance of a contract between the data subject and the controller;
- the transfer is necessary for the performance of a contract concluded in the interest of the data subject and between the controller and another natural or legal person;
- the transfer is necessary for the public interest;
- the transfer is necessary for the establishment, exercise, or defence of legal claims; or
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the subject is physically or legally incapable of giving consent;

In all this, the data subject is expected to have been given clear warnings of the principles of data protection that are likely to be violated in the event of the transfer.

**Cloud Computing**

The NITDA recently proposed and published a draft National Cloud Computing Policy 2019 ('the Policy'). The policy defines Cloud Computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service interaction.

The Policy provides for three kinds of cloud-based service models:

- Software as a Service (SaaS);
- Platform as a Service (PaaS); and
- Infrastructure as a Service (IaaS).

Whereas the three internationally recognised deployment models for cloud services are:

- private cloud: cloud infrastructure provisioned for exclusive use by a single organisation;
- public cloud: cloud infrastructure provisioned for open use by the general public; or
- hybrid cloud: cloud infrastructure which is a composition of two or more distinct private and public cloud infrastructure.

In terms of application, the Policy is not stated to apply to FIs directly and instead applies to:

- all federal, state and local public institutions; and
- all corporations fully or partially owned by the Federal Government in Nigeria, in so far as data generated by these intuitions constitute data that may be regarded as 'government data'

The Policy will take effect upon its publication.

# 8. BREACH NOTIFICATION

There is no express provision in the NDPR to report breaches. NITDA may, however, take the view that the obligation for an audit to be conducted on a company's procedure for reporting privacy violations in Article 4.1(5) of the NDPR equally imposes an obligation on the company to report privacy breaches.

# 9. ENFORCEMENT

### 9.1. Penalties issued by the Framework

According to the Framework, the CBN shall adopt effective mechanisms to support the enforcement of consumer protection regulations. These mechanisms will be backed by other industry regulations.

For enforcement purposes, the CBN will make investigations when necessary, and findings shall form the basis for management decisions.

Where a breach has occurred, some of the sanctions the CBN may impose include:

- refund to customers in line with relevant regulations issued by the CBN;
- letter of apology;
- restriction on activities;
- suspension from inter-bank activities;
- suspension/withdrawal of foreign exchange dealership license;
- denial of approvals;
- publication of infractions and sanctions;
- monetary penalties;
- product recall;
- adverts cancellation;
- warning letters to management/board;
- suspension/removal of board/management staff/employees;
- referral to law enforcement agencies for prosecution;
- revocation of banking license; and
- other sanctions deemed appropriate.

### 9.2. Penalties issued by NDPR

According to the NDPR, any person subject to it that is found to be in breach of the data privacy rights of any data subject will be liable in addition to any other criminal liability, to the following:

- in the case of a data controller dealing with more than 10,000 data subjects, payment of the fine of 2% of annual gross revenue of the preceding year or payment of the sum of NGN 10 million (approx. €25,000) whichever is greater; and
- In the case of a data controller dealing with less than 10,000 data subjects, payment of the fine of 1% of the annual gross revenue of the preceding year or payment of the sum of NGN 2 million (approx. €5,000) whichever is greater.

### 9.3. Penalties issued by the Cybercrimes Act

The Cybercrimes Act prescribes a long list of penalties and monetary fines that will be paid to the courts in the event of an offence. Some of these include:

- unlawful access to a computer, punishable with imprisonment of ten to 15 years, without an option of fine; and
- computer related forgery which involves intentional manipulation of data by accessing a computer or other network and altering, deleting or supressing data, in order to render the said data inauthentic. Upon conviction, this offence is punishable with imprisonment for a term of three years, a fine of NGN 7 million (approx. €18,000), or both.

## 10. ADDITIONAL AREAS OF INTEREST

Not applicable.

ABOUT THE AUTHORS

**Davidson Oturu**

*Aelex*

Davidson is a Partner in AELEX, a law firm with offices in Nigeria and Ghana, and works in the firm's corporate/commercial, intellectual property, technology, media, and telecommunications (TMT) practice groups.

He regularly counsels on matters related to technology, data protection, and intellectual property rights. He also advises on various trans-border issues relating to ICT, including but not limited to Financial Technology (FinTech), Cybersecurity, Digital Signature, Digital Rights Management (DRM) Data Protection & Privacy. He was recently appointed by the Securities & Exchange Commission (SEC) to the committee charged with the responsibility of setting up a framework for the use of FinTech in the Capital Markets.

Among other things, he advises foreign investors seeking to establish entities in Free Trade Zones and also advises various multinationals on the framework for foreign direct/portfolio investments in Nigeria. As a Lead Adviser to several multinationals, he ensures that their businesses are compliant by assisting them on corporate immigration formalities that are required for doing business in Nigeria. His regulatory advisory work includes the provision of legal support to technical advisory groups funded by the USAID and DFID that are aimed at providing high-level support to Federal and State Government agencies on their Public Private Partnership (PPP) programmes.

He was recognised by the World Trademarks Review, in its 2019 rankings, as one of the world's leading 1,000 trademarks practitioners. He was also recognised as a 'next generation lawyer' by the Legal 500 in its 2019 rankings.

doturu@aelex.com

RELATED CONTENT

LEGAL RESEARCH

**Anti-Money Laundering and Counter-Terrorist Financing Guidelines to Insurers**

LEGAL RESEARCH

**Anti-Money Laundering Guidelines to CMSA Licensees**

LEGAL RESEARCH

**The Anti-Money Laundering (Electronic Funds Transfer and Cash Transactions Reporting) Regulations, 2019**

LEGAL RESEARCH

**Outsourcing of Functions by Entities Licensed under the Protection of Investors (Bailiwick of Guernsey) Law, 1987**

NEWS POST

**Singapore: MAS announces framework for responsible use of AIDA in financial sector**