ÆLEX

ARTICLE SERIES

THE EFFECT OF NIGERIA'S DATA PROTECTION REGIME ON OPEN BANKING

MAY 2021

www.aelex.com

INTRODUCTION

Historically, the banking relationship between a bank and its customer is a private one. The novelty of open banking lies in its audacious challenge to this historical model by promoting the sharing of the customer's banking data with 'trusted' third parties [1]

Open banking is an emerging financial services model that focuses on the portability and open availability of customer data held by financial institutions [2]. It involves opening up banking systems, particularly customer data, to third parties to allow them provide services directly to customers. This access to data and functionality gives challenger banks, financial technology companies (FinTechs) and other players in the financial sector the opportunity to develop innovative financial products and services, promote competition and improve customer experience.

The underlying reasoning powering the development of open banking proceeds on the basis that customers own their banking data and should therefore reap the benefits from such ownership by having it shared in ways that are beneficial to the customers.

Open banking operates by granting Third Party Providers (TPPs) open access to consumer banking, transactions and other financial data from banks and non-bank financial institutions through the use of Application Programming Interface (API).

It therefore enables the sharing of financial data across multiple financial institutions. This unlocks possibilities for TPPs as they will have the opportunity to access the enormous data being held by traditional financial institutions.

The potential benefits notwithstanding, without appropriate legal protections, the proposed dramatic increase in collection and sharing of personal information will operate to the detriment of consumers by exposing them to proportionately greater risks from the unauthorized and fraudulent use of their personal information. Fortunately, there has been a rising awareness in data protection and privacy in Nigeria over the last few years with the introduction of the Nigeria Data Protection Regulation, 2019 (NDPR) and the Data Protection Implementation Framework (DPIF).

In this article, we explore the effects and implications of the NDPR on the implementation and operation of open banking in Nigeria.

[1]James Black & Krista Koskivirta, "Open Banking - What is it and what is it good for?" (2018) Annual Banking Law Update 39.
[2]Ana Badour & Domenic Presta, "Open Banking: Canadian and International Developments" (2018) 34:1 Banking and Finance Law Review 41.

OPEN BANKING IN NIGERIA

The regulatory approaches towards open banking can be broadly classified into three namely, mandatory, supportive and neutral approaches. In a mandatory jurisdiction, regulators pass legislation compelling the adoption of open banking practices, supportive jurisdictions merely facilitate open banking without mandating it while neutral jurisdictions are characterized by the absence of regulatory statements on open banking.

Prior to February 2021 when the Central Bank of Nigeria (CBN) released the Regulatory Framework for Open Banking in Nigeria (the Framework), Nigeria was a neutral jurisdiction. However, with the release of the Framework, Nigeria became a supportive jurisdiction as the Framework does not mandate but simply attempts to facilitate open banking.

The trichotomy of regulatory approaches is relevant because it dictates the applicable legal regime in a jurisdiction.

For instance, in mandatory jurisdictions (like Australia), TPPs are regulated as data recipients and the legal framework is expanded to include TPPs' rights and duties in accessing customer banking information. In contrast, in supportive (like Nigeria) and neutral jurisdictions, a customer's rights over his/her banking data is governed by pre-existing banking law/regulation and by existing data protection legislation/regulation.

THE NIGERIA DATA PROTECTION REGULATION (NDPR), 2019

The NDPR was issued by the National Information Technology Development Agency (NITDA) to address emerging issues in data protection and privacy. It was issued to regulate those who have access to and control people's data (Data Controllers) particularly due to the amount of data created by users of the internet and stored on it. As such, security of personal data became a national concern as companies, organizations and hackers continually seek to exploit the information for commercial and malicious purposes.

Prior to the NDPR, there existed provisions in a few laws which protected certain classes of data or information from unlawful use. However, unlike the NDPR, these provisions were inadequate and ineffective in imposing sanctions and ensuring compliance in the event of a data breach.

Although a subsidiary legislation, the NDPR is currently Nigeria's most comprehensive law on data protection. It contains various provisions regulating the collection and processing of data in Nigeria. The provisions of the Regulation mirror the Fair Information Practice Principles (FIPP) which are generally considered foundational principles of privacy policy.

The Regulation seeks to safeguard the rights of natural persons to data privacy [3] and applies to all transactions intended for the processing of personal data of natural persons who are Nigerians, whether in Nigeria or outside the country [4].

Consequently, banking data of natural persons (Nigerians) fall under the purview of the Regulation and the implementation of open banking in Nigeria must therefore be carried out in compliance with its provisions.

IMPLICATIONS OF THE NDPRON THE OPERATION OF OPEN BANKING IN NIGERIA

Below are some of the ways the NDPR impacts the operation of open banking in Nigeria.

a.Consent

Consent is one of the cardinal principles of data rights and is a legal basis for processing personal data. The NDPR provides for strict guidelines for the obtainment of consent from Data Subjects [5]. It states that no data shall be obtained except for a specific purpose made known to the data subject [6]. The procurement of consent must also be without fraud, coercion or undue influence [7]. The NDPR further places an obligation on the Data Controller to demonstrate that the data subject had consented to the processing [8]

[3]Article 1.1 of the Nigeria Data Protection Regulation, 2019.
[4]Article 1.2 (a) & (b) of the Nigeria Data Protection Regulation, 2019.
[5] Data subject refers to any natural person who can be identified, directly or indirectly, through an identifier such as a name, an ID number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity.
[6]Article 2.3 (1) of the Nigeria Data Protection Regulation, 2019.
[7]Article 2.3 (2) of the Nigeria Data Protection Regulation, 2019.
[8]Article 2.3 (2) (a) of the Nigeria Data Protection Regulation, 2019.

The data subject should also be informed of his right to withdraw his consent at any given time [9].

It is therefore important for participants in open banking who collect data to get specific consent from Data Subjects about sharing of the data collected. Furthermore, it is critical that any customer consent to data practices under open banking is voluntary, explicit, and revocable.

b. Purpose

The NDPR provides that personal data shall only be collected and processed in accordance with the specific, legitimate and lawful purpose consented to by the customer/data subject. Therefore, the NDPR envisages that at the point of obtaining consent, the purpose for which the data is being collected is clearly stated and made known to the customer. [10] Participants in open banking in Nigeria will therefore have to inform their customers at the point of obtaining consent that same will be shared with TPPs for the achievement of open banking goals or objectives.

The Regulation further mandates that whenever the Controller intends to further process personal data for a purpose other than that for which the data was collected, the Controller shall provide the data subject prior to that further processing with information on that other purpose, and with any relevant further information [11]

This is relevant in the case of data obtained by the Controller prior to the implementation of open banking since at the time of collection, sharing with third parties for the purpose of open banking was not stated as one of the purposes for collection. Hence, Controllers will have to inform data subjects of this new purpose.

c. Privacy Policy

The purpose of a Privacy Policy is to notify the individual of what an organization is collecting, using and sharing regarding their data.
The NDPR mandates all medium through which personal data is being collected or processed to display a conspicuous privacy policy that the class of targeted data subjects can understand. The privacy policy shall in addition to any other relevant information contain information such as what constitutes data subject's consent, description of collectable personal information, purpose of collection of personal data etc [12]

[9]Article 2.3 (2) (c) of the Nigeria Data Protection Regulation, 2019.
[10]Article 2.1 (1) (a) of the Nigeria Data Protection Regulation, 2019.
[11]Article 3.1 (7) (m) of the Nigeria Data Protection Regulation, 2019.
[12]Article 2.5 of the Nigeria Data Protection Regulation, 2019.

Importantly, by law, an organization that publishes its practices must adhere to them and ensure commitment so as to avoid liability of deceptive practices.

Privacy policies or notices do not relate specifically to open banking as Controllers would ordinarily have had to comply with the requirement by virtue of collecting and processing data without necessarily sharing. However, for entities with interest in open banking, the aspects of their privacy policies, like purpose of collection of data, access of third parties to personal data and purpose of access have to be updated to reflect the necessary changes.

d. Due Diligence

The NDPR places on all parties to a data processing agreement (other than the data subject), the responsibility of taking necessary measures to ensure that other parties do not have a record of violating or abusing data. The NDPR also provides that data processing by a third party shall be governed by a written contract between the third party and the Data Controller.

Accordingly, any person engaging a third party to process the data obtained from data subjects shall ensure adherence to the Regulation. [13]

Consequently, every Data Controller is liable for the actions of third parties who handle the personal data of data subjects under the NDPR [14]. These set of provisions are particularly apposite for the open banking scenario as they place responsibility on the traditional institutions that are in position to share customer data to conduct extensive due diligence and vet all parties before onboarding them as they will be liable for the actions of all third parties they grant access.

e. Security

The NDPR requires anyone involved in data processing or the control of data to develop security measures to protect data; such measures include protecting systems from hackers, setting up firewalls, storing data securely, 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 staff. [15]

[13]Article 2.7 of the Nigeria Data Protection Regulation, 2019.
[14]Article 2.4 (b) of the Nigeria Data Protection Regulation, 2019.
[15]Article 2.6 of the Nigeria Data Protection Regulation, 2019.

The NDPR further requires that personal data is secured against all foreseeable hazards and breaches such as theft, cyberattack, viral attack, dissemination, manipulations of any kind, damage by rain, fire or exposure to other natural elements. [16]

If open banking achieves its objective of making customer data sharing easier, it will be held by more entities and more points of storage will increase the number of potential stages at which data can be compromised. It is therefore not enough for data controllers and processors to lawfully obtain data; they must also ensure that they develop standard security systems to protect the data in their possession. The responsibility of putting in place protective infrastructure is placed on the Data Controllers and they will have to develop competence to deal with all foreseeable breaches. In an open banking environment, the risk for Data Controllers is multiplied and entities looking to participate must bear this in mind and put in place the necessary measures.

f. Data Subject's rights

The right of a data subject to object to the processing of his data is safeguarded by the NDPR. This is relevant in relation to open banking as some data subjects may have reservations and lack of trust in the notion of their personal data being shared with third parties. This class of persons shall have the right to object to such processing and be provided with a mechanism for objection at no cost to them [17]

The NDPR also grants data subjects the right to request from the Controller access to and rectification or erasure of personal data [18] The NDPR further requires that the Controller shall communicate any rectification or erasure of personal data to each recipient to whom the information had been disclosed, unless this proves impossible or involves disproportionate effort. The Controller shall inform the data subject about those recipients if the Data Subject requests it. [19]

[16]Article 2.1 (1) (d) of the Nigeria Data Protection Regulation, 2019.
[17]Article 2.8 of the Nigeria Data Protection Regulation, 2019.
[18]Article 3.1 (7) (h) of the Nigeria Data Protection Regulation, 2019.
[19]Article 3.1 (13) of the Nigeria Data Protection Regulation, 2019.

Hence, when on the data subject's demand, data is rectified or erased in an open banking scenario, the Controller is obligated to communicate such rectification or erasure to all parties with whom the data has been shared.

The NDPR also supports data subjects' right to data portability and states that the data subject shall have the right to have personal data transmitted directly from one controller to another, where technically feasible. [20] This right is very relevant to open banking as it implies that if the data subject requests that his/her data be shared with a specified third party, the Controller is obligated to honour such a request.

g. Compliance

The NDPR recommends some actions to be taken by data controlling entities to improve their chances of complying with the requirements under the Regulation.

It endorses Data Protection Compliance Organizations (DPCOs) which are data protection professionals established by the NDPR to help organizations ensure compliance [21]. Thus, where an organisation processes personal data of 1,000 data subjects in 6 months, or 2,000 data subjects in 12 months, it will be required to engage a DPCO to conduct an audit on its processes and file the report with NITDA.

The NDPR also encourages entities to conduct data protection trainings for their staff by inviting experts such as DPCOs to anchor the process [22]. This way, their employees, especially those specifically responsible for processing data, would be enlightened on how to prevent data breaches.

These directives on ensuring compliance are particularly relevant for participants in open banking in light of the increased risks and it will be reasonable to adopt the recommendations to limit exposure.

[20] Article 3.1 (15) of the Nigeria Data Protection Regulation, 2019
[21]Article 4.1 (4) of the Nigeria Data Protection Regulation, 2019.
[22]Article 4.1 (3) of the Nigeria Data Protection Regulation, 2019.

h. Penalty

The provisions and obligations set out in the Regulation have been backed by penalty for default to ensure compliance. Accordingly, any person subject to the NDPR who is found to be in breach of the data privacy rights of any Data Subject shall be liable, in addition to any other criminal liability, to, 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 10 million Naira, 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 2 million Naira, whichever is greater. [23]

Considering the implementation of open banking's greater risk of resulting in a breach, it is important that participants take necessary steps to ensure absolute compliance with the provisions of the Regulation so as to avoid penalties.

[23]Article 2.10 of the Nigeria Data Protection Regulation, 2019.

Conclusion

The benefits of open banking such as enablement of innovative products and services, competition and better customer experience are undoubtedly positives and strong arguments in favour of its adoption. However, at the core of its proposition is wide scale data sharing which raises serious concerns about data privacy and protection. Participants will therefore have to comply strictly with extant laws if the implementation and operation of open banking is to be a success.

ÆLEX

Davidson Oturu
(Partner, AELEX)

Mubaraq Popoola
(Associate, AELEX)

For further information, please contact:

Davidson Oturu
(doturu@aelex.com)

Frances Obiago
(fobiago@aelex.com)

Florence Bola-Balogun
(fbola-balogun@aelex.com)

Oyeyosola Diya
(odiya@aelex.com)

Opeyemi Adeleke
(oadeleke@aelex.com)

Kehinde Takuro
(ktakuro@aelex.com)

ÆLEX is a full-service commercial and dispute resolution firm. It is one of the largest law firms in West Africa with offices in Lagos, Port Harcourt and Abuja in Nigeria and Accra, Ghana. A profile of our firm can be viewed here. You can also visit our website at www.aelex.com to learn more about our firm and its services.'

CONTACT DETAILS

LAGOS, NIGERIA

4th Floor,
Marble House
1, Kingsway Road, Falomo
P. O. Box 52901, Ikoyi
Lagos, Nigeria

Telephone: (+ 234 1) 2793367; 2793368
4736296, 4617321-3;
Facsimile: (+ 234 1) 2692072; 4617092
E-mail: lagos@aelex.com

PORT HARCOURT, NIGERIA

2nd Floor,
Right Wing UPDC Building
26, Aba Road
P.O. Box 12636, Port Harcourt
Rivers State, Nigeria

Telephone: (+234 84) 464514, 464515
574628, 574636
Facsimile: (+234 84) 464516, 574628
E-mail: portharcourt@aelex.com

ABUJA, NIGERIA

4th Floor,
Adamawa Plaza
1st Avenue, Off Shehu Shagari Way
Central Business Area
FCT Abuja, Nigeria

Telephone: (+234 9) 8704187, 6723568,
07098808416
Facsimile: (+234 9) 5230276
E-mail: abuja@aelex.com

ACCRA, GHANA

7th Floor, Suite B701
The Octagon
Accra Central, Accra
P.M.B 72, Cantonment Accra, Ghana

Telephone: (+233-302) 224828, 224845-6
Facsimile: (+233-302) 224824
E-mail: accra@aelex.com