The AELEX FinTech Interview Segment

ÆLEX

FINTECH CENTRE

DATA PROTECTION FOR FINANCIAL TECHNOLOGY COMPANIES OPERATING IN NIGERIA

INTERVIEWEE- OPEYEMI ARAROMI ⟶

DATA PROTECTION FOR FINANCIAL TECHNOLOGY COMPANIES OPERATING IN NIGERIA

Opeyemi Araromi is an associate in the Technology, Media and Telecommunications practice group at AELEX. She provides legal advisory services to Nigerian and international corporate structures on data privacy and protection, and also provides regulatory compliance and company secretarial services to technology, media and telecommunication companies.

In her spare time, she can be found seeking new adventures, analysing Nigeria's entertainment sector and giving back to her community as much as she can.

INTERVIEWEE - OPEYEMI ARAROMI

Now to our questions for Opeyemi.

1. Opeyemi, how important is data protection for financial technology ("fintech") companies?

Data protection has been a major discourse amongst stakeholders worldwide. The rise in the use of technology has particularly made personal data easily accessible. The concept of digital footprint leaves the personal data volatile, making it susceptible to use by individuals and organisations without the permission of data owners. Data exchange has also become an intricate part of commercial transactions, with data protection being a risk issue which most companies put into consideration before contracting with other companies or institutions. The governments of nations, Nigeria inclusive, have thus risen to the task of protection of personal data, which is a constitutionally recognised right.

This right has evolved over the years and is now being codified in different pieces of legislation. At the moment, the most relevant legislative instrument on data protection is the Nigerian Data Protection Regulation (NDPR) issued by the National Information Technology Development Agency ("NITDA").

By the nature of their operations, fintechs process the personal data of their consumers when effecting transactions on their behalf. All fintech companies are therefore required to comply with the data protection regulations when handling personal data to avoid penalties and default from non-compliance.

2. What are the laws that govern data protection in Nigeria?

The laws that govern data protection and affect fintech companies in Nigeria below:

• Constitution of the Federal Republic of Nigeria 1999 (as Amended)

•The Freedom of Information Act 2011

•The Cybercrime (Prohibition, Prevention, etc) Act 2015

•Advanced Fee Fraud and Other Fraud Related Offences Act 2006

•CBN's Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) Policy and Procedure Manual

•CBN's Consumer Protection Framework ("Framework")

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

•The Consumer Code of Practice Regulations 2007 The Nigeria Data Protection Regulations 2019

3. Is it compulsory for fintech companies to comply with the Nigeria Data Protection Regulation (NDPR)?

Yes, it is compulsory for fintechs to comply with the NDPR. Under the NDPR, there are certain categories of persons that are referred to as data controllers.

The NDPR defines a data controller as a person who either alone or jointly with other persons or a statutory body, determines the purposes for and the manner in which personal data is processed or is to be processed.

As fintech companies have access to the data of individuals and process them in order to execute transactions on their behalf, they will be deemed as data controllers on whom compliance obligations are imposed.

4. Are there any penalties for non-compliance with data protection laws in Nigeria?

Yes, there are different penalties for non-compliance with the data protection laws. We can break them into different categories of penalties.

<u>Penalties under the Framework</u>

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 licence; and
•other sanctions deemed appropriate.

<u>Penalties issued by NDPR</u>

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. $21,053[1]) 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. $4, 215) whichever is greater.

<u>Penalties issued by the Cybercrimes Act</u>

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

[1] Exchange rate of Naira to dollars as at 20 January 2021.

• *computer related forgery which involves intentional manipulation of data by accessing a computer or other network and altering, deleting or suppressing 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.$14,737), or both.*

5. Are there any penalties for late compliance to data protection laws in Nigeria?

At the moment, the extant laws do not consider late compliance and would issue a penalty in the event of non-compliance.

6. What kind of data is required by the NDPR to be protected?

The NDPR protects personal data. Personal data is information that relates to natural persons. It can be used to identify an individual directly or indirectly. It is also defined as "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 and others. [2]"

7. What specific steps must be taken by a fintech company in relation to data protection in Nigeria?

Please see the obligations required of a fintech company below:

i. ***Establish the legal basis for processing any personal information.***

ii. ***Display privacy policy*** *on every medium through which personal data is being collected or processed.*

iii. ***Design a data protection compliance system****: develop security measures to protect the data collected;*

iv. ***Designate a Data Protection Officer****;*

v. ***Develop the continuous capacity of DPOs and other members of staff****.[3] It is advisable that the role of a DPO is outsourced to a competent and verifiable firm, with supervision by a top official of the company. The DPO can further train other members of staff.*

vi. ***Conduct Data Protection Impact Assessment ("DPIA"):*** *A DPIA is a process which aids in the identification of data processing risks of either a particular project which involves processing of personal data or the organisation's general processes.*

A typical record of a DPIA should include the following:

- The details of the data controller and the DPO.
- The need for a DPIA for the data processing. This would entail a description of the data processing by the company. If for a specific project or work, it should include what the project aims to achieve.
- The nature of the processing/data flow should be described.
- The organisation's consultation process with relevant stakeholders should be stated. This would cover how the company intends to seek individuals' views - as well as the company's plans to consult information security experts.
- Compliance and proportionality measures should be stated. This would involve stating the lawful basis for processing, how the company intends to ensure data quality and data minimization, the information to be given to individuals, how the company intends to help support their rights, the measures to be taken to ensure processors comply and the safeguarding of international transfers.
- Identification and assessment of risks and potential impact on individuals.

ii. ***Enter/Update agreement with third party processors*** *to ensure compliance with the NDPR.*

iii. ***Carry out an audit of its data protection practices annually.***

[2] Section 1.3 of the NDPR.
[3] The NDPR is silent on training other members of staff, the inclusion is from the DPIF

8. What is a data protection audit report?

Audits are investigations or examinations of records, process and procedure of Data Controllers and processors to ensure they are in compliance with the requirements of the NDPR. Data Audits are carried out by Data Protection Compliance Organizations (DPCOs). DPCOs, on behalf of NITDA, monitor, audit and conduct training on data protection compliance to all Data Controllers. It is important to state that AELEX is a DPCO and can assist fintech companies to comply with data protection laws and file a data protection audit report with NITDA.

***9.* Is there a timeline for filing the data protection audit report?**

On an annual basis, a Data Controller who processes the Personal Data of more than 2000 Data Subjects in a period of 12 months shall, not later than the 15th of March each year, submit a summary of its data protection audit to NITDA.[4]

10. What steps does a fintech company need to take to disclose personal data in our possession or is this even permissible?

You may disclose personal data in your possession where you have obtained consent of the data subject concerned or complied with any of the legal basis for processing personal data.

11. Are there permissible grounds for disclosing personal data without consent? For instance, when an employee tests positive for COVID-19.

Yes, you may disclose personal data without consent on the basis that the data being processed:
• is for the performance of a contract;
• is required for compliance with a legal obligation;
• is required for protection of the vital interest of a data subject or another natural person; or
• is necessary for the performance of a task carried out in the public interest.[5]

12. What should a fintech company's privacy policy contain?

An organisation's privacy policy must be simple and written in plain English so it is understandable to data subjects. Also, in accordance with the NDPR, an organisation's data policy must at the minimum, contain the following:

• what constitutes the Data Subject's consent;
• description of collectable personal information;
• purpose of collection of personal data;
• technical methods used to collect and store personal information, cookies, JWT, web tokens etc.;
• access (if any) of third parties to personal data and purpose of access;
• a highlight of the standard data protection principles;
• available remedies in the event of violation of the privacy policy;
• the time frame for remedy; and
• any limitation clause, provided that no limitation clause shall avail any Data Controller who acts in breach of the stated data protection principles.

13. Are there any other specific data protection obligations required of financial technology companies since many of them now have their staff working remotely?

This is a topic that is of recent concern amidst the global pandemic. Accordingly, AELEX has extensively addressed this topic in its article – "Data Privacy Checklist for Working Remotely in the Wake of Covid-19"

14. Does monitoring employees' social media accounts, obtaining information from their social media and making use of said information infringe any data privacy laws in Nigeria?

Yes, it does. Please note that an employee is also a data subject with rights to data privacy.

15. Is there any additional information that fintech companies should take note of to ensure that they comply with data protection laws in Nigeria?

Such additional information can be found in this article . Thank you.

[4] Article 4.1.7 of the NDPR
[5] Section 2.2 of the NITDA Data Protection Regulation.

(DISCLAIMER: This publication is not intended to provide legal advice but to provide information on the matter covered in the publication. No reader should act on the matters covered in this publication without first seeking specific legal advice.)

CONTACT DETAILS

LAGOS, NIGERIA

7th 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

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

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

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

www.aelex.com