



**THE CHARTERED INSTITUTE OF BANKERS OF
NIGERIA CENTRE FOR FINANCIAL STUDIES
(CIBNCFS)**

**COMMUNIQUE ISSUED
AT THE END OF THE
BREAKFAST SESSION ON MANAGING THE “NEW
OIL” - DATA PROTECTION AND MANAGEMENT
STRATEGIES FOR THE NIGERIAN BANKING
SECTOR**

**HELD AT THE BANKERS HOUSE
VICTORIA ISLAND, LAGOS**

DATE: JULY 18, 2019

Background

The Breakfast Session on Managing the “New Oil”: Data Protection and Management Strategies for the Nigerian Banking Sector was held on Thursday, July 18, 2019 at the Bankers House, Victoria Island, Lagos. The objectives of the Session were, among other things to; give participants a better understanding of the Nigeria Data Protection Regulation, 2019; discuss modalities for implementation of the Regulation, the role of all stakeholders in the data ecosystem, the impact of the regulation on innovation and profitability drives and best practices in data management and protection with lessons for the Nigerian Banking & Finance Industry.

In his welcome address, the President/Chairman of Council of The Chartered Institute of Bankers of Nigeria, Uche M. Olowu, Ph.D, FCIB noted that data management and protection issues should be of great concern to us all. He further explained that breaches in data protection guidelines and laws have resulted in reputational damage and a higher risk of illicit activities such as money laundering and identity fraud. He also stressed the importance of consumer consent or rather “Consent Fatigue” where organizations seeking legitimate use of data serve customers with several consent notifications or forms and as a result, customers, without taking the time to fully understand these forms or notifications indicate agreement. He stated that the banking community must display exemplary ethical conduct in the management of personal information and act as shining beacons to other industries.

Dignitaries Present

Office Holders

- a.) Uche M. Olowu, Ph.D, FCIB, President/Chairman of Council, CIBN
- b.) Prof. Pius Olanrewaju, National Treasurer, CIBN

Facilitators

- c.) Prof. Rosaline Opeke, Professor of Information & Data Resources, Babcock University
- d.) Prof Olalekan Asikhia, Director, CIBN Centre for Financial Studies
- e.) Mr Seyi Adenmosun, Head, Operations, Nigeria Inter-Bank Settlement Systems Plc
- f.) Mr Babatunde Okeniyi, Executive Director, Unified Payments Nigeria
- g.) Mr Adeniyi Adegbonmire, SAN, Senior Partner, Aluko & Oyebode
- h.) Mr Deji Oguntonade, Divisional Head, FinTech & Innovation, Guaranty Trust Bank
- i.) Dr Raphael Yemitan, Senior Manager, Advanced and Predictive Analytics, PwC Nigeria

Keynote Address & Presentation

Keynote Address

The Keynote Address was delivered by Dr. Isa Ali Pantami, Director General/Chief Executive Officer, National Information Technology Development Agency (NITDA), ably represented by Mr Adejube

Olayinka, Director, Standard Guidelines & Framework, National Information Technology Development Agency (NITDA). The address read by Mr. Olayinka explained that the Nigeria Data Protection Regulation (NDPR) strives to bring sanity to the handling of data as it is a critical resource for transformation of economies. The NDPR also addresses all issues and safeguards, necessary for the handling of Data belonging to Nigerians - processed either within its shores and/or transmitted outside.

He also explained that businesses can benefit from operating in compliance as transparency and best practice implicitly enshrined in the regulation begets business growth and customer confidence. Furthermore, costs associated with a data breach such as paying back any money taken as a result of the breach, legal costs, compensating affected customers, share-value plummeting and having to pay for the right protection, could be avoided.

Keynote Presentation

Mr Olufemi Daniel, Desk Officer (Data Protection, NITDA) gave a Presentation on the NDPR: Implications for the Nigerian Banking Industry

Key points of the presentation were as follows:

- The right to be left alone is a constitutional concept that arose from Justice L.D Brandei - *Olmstead v. US* 277 US.438 (1928).
- The right to Privacy was promoted to limit the intrusion of government on private life. It covers private correspondence, email and internet use, medical record, personal data, sexual orientation etc.
- The Nigeria Data Protection Regulation (NDPR) is Nigeria's current national law on data protection. The scope of the NDPR covers:
 - All transactions intended for the processing of Personal Data
 - All natural persons residing in Nigeria or residing outside Nigeria who are citizens of Nigeria
- In the regulation, there are six basis in which data could be held legally. They are as follows:
 - **Consent of Subject/Customer** – the data subject (customer) has given consent to the processing of his or her personal data for one or more specific purposes
 - **Vital Interest of Data Subject** - processing is necessary in order to protect the vital interests of the data subject
 - **Public Interest** - 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 data controller
 - **Legitimate Interest** - processing is necessary in order to protect the vital interests of the data subject or of another natural person and
 - **Contract** – processing is necessary for the performance of a contract to which the Data Subject is a party or in order to take steps at the request of the Data Subject prior to entering into a contract
 - **Legal Compliance** - processing is necessary for compliance with a legal obligation to which the Data Controller is subject
- Every bank needs at least one of the listed basis above for holding personal information

- Every data subject has the right to grant or retrieve consent to data use
- The NDPR does not mandate private businesses to host data only on local servers, although this is highly encouraged. Government data as well as critical national data in the custody of private organisations must however be hosted in-country

2.0 Highlights and Recommendations

A. Highlights

The following were highlights of the session:

Data Management & Protection

- The organizational culture of a company comes into play when considering data protection strategies. Staff who handle data must be trained to understand the focus of the company and the importance of handling data discreetly.
- Incentives to encourage compliance with data protection regulation must be developed. This is because policies for prevention are better than punishment.
- Data privacy is a constitutional right which cannot be breached at will. Consumers/customers have a right to awareness of what their personal information would be used for and if it would be transferred to third parties.
- The period of storage of personal data in a bank after a customer may have closed an account depends on the following:
 - Regulation – the predetermined time in which data is to be warehoused
 - Cost of data – the cost of deleting the data
- Regulators must catch up with the developments/opportunities currently on ground in the financial services industry. For example, open banking employs the use of open data – that is data are freely available to everyone to use and republish as they wish, without restrictions from copyright, patents or other mechanisms of control.
- The California Consumer Privacy Act (CCPA), adopted on 28 June 2018, is seen as laying upon or an extension of the European Union's (EU) General Data Protection Regulation (GDPR) and is currently one of the most comprehensive data privacy regulations in the US.
- On June 25, 2019, the Central Bank of Nigeria (CBN) issued an exposure draft on Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers. This framework makes provisions for the protection of customer data and cybersecurity governance.

Data Governance Systems: The Data Governance Maturity Model (DGMM)

- The Data Governance Maturity Model is a strategy which helps organizations understand their current level of data management. More importantly, the model can identify a path for growth in the future.
- Strategies should go beyond data management and protection. In addition, each organization which handles personal data should have a system in place which would ensure data governance.

- It is important for an organization to identify its current stage of operation. Companies that plan their evolution in a systematic fashion gain over those that are forced to change by external events. The Data Governance Maturity Model can however help control that change by determining what stage is appropriate for the business, how and when to move to the next stage.
- The CIBN Centre for Financial Studies would work with banks and other financial organizations to ensure the optimal implementation of the model.

B. Recommendations

Recommendations for individual agents in ensuring data management, privacy and protection are outlined below as follows:

National Information Technology Development Agency (NITDA)

- The National Data Protection Regulation should be further developed for robustness. However, regulators must ensure that businesses are not stifled in the process.
- NITDA should learn from the CBN in introducing regulations. The typical process for CBN in introducing regulations involves stakeholder engagements across industries concerned, public and private sector engagements as well as the development and final adoption of exposure drafts.
- A dispute resolution team should be developed to settle cases of data breaches across various industries
- Organize several more Fora in the pilot phase of the dispute resolution.
- A more robust response to data breaches should be developed in the NDPR guidelines. That is, a strong deterrent to breaches in data privacy should be developed so as to ensure that data breaches are not easy to accomplish.
- NITDA should ensure that regulation can shield against possible dangers of emerging opportunities such as open banking.

Financial Institutions & Businesses

- Behavioral characteristics of those handling sensitive data should be scrutinized
- Data champions and stewards who would monitor data use from one process (collection, transfer, usage), to the other should be employed
- There should be adequate training and retraining for these agents as well as data controllers handling sensitive data.
- The IT, Compliance and Legal departments should work together to determine how to manage data in every organizations.
- It is important for individuals and organizations to gain a better understanding of processes in which data breaches could occur e.g. in data collection, transfer or usage.
- Businesses should consider employment of The Data Governance Maturity Model (DGMM)
- organisations should work with the CIBNCFS in implementation of the DGMM model

- Banks must be more stringent when considering third party engagements. Such engagements must be scrutinized more thoroughly in order to reduce the likelihood of data breaches.
- Ensure to adopt and implement NDPR Regulatory Checklist

The Chartered Institute of Bankers of Nigeria (CIBN)

- Further sensitize bankers on the need for data management and governance strategies
- Work with banks to implement the Data Governance Maturity Model

3.0 Conclusion

The session was well attended with delegates from regulatory institutions (the Central Bank of Nigeria), deposit money banks, microfinance banks, insurance banks, FinTechs and SMEs in attendance. While data management and protection strategies were outlined during the session, stakeholders were also advised to seek data governance systems.

The faculty displayed excellent mastery of the subject matter and the contributions by participants to the discussions were insightful.

Prof. Olalekan Asikhia

Director

CIBN Centre for Financial Studies