A Quick Guide on the Data Protection Regime in Nigeria

Introduction

As data becomes a highly sought commodity, more and more people are concerned about how their data is stored, processed, and transmitted. The advent of Big Data, availability of advanced data analytics tools, and surge in surveillance activities have transformed into a mass resuscitation of the desire to have data collected and processed only on legal bases and for specified purposes.

Although significant progress has been made in recent time, there is currently no dedicated, principal legislation on data protection in Nigeria. In fact, until early 2019 when the National Information Technology Development Agency (NITDA) issued its Data Protection Regulation, provisions on data protection were few, incomprehensive, and dispersed in general and sector-specific legislation.

This essay examines the legal framework for data protection in Nigeria.

The Nigeria Data Protection Regulation 2019 (NDPR/Regulation)

On 25 January 2019, the NITDA issued the NDPR. Currently the most-encompassing legislation on data protection in Nigeria, the NDPR is hailed as a game changer—it applies to all transactions intended for the processing of personal data, and to the actual processing of personal data in respect of natural persons residing in Nigeria or residing outside Nigeria but of Nigerian descent.

To give Data Subjects some control over their data and ensure that personal data is processed strictly based on lawful bases, the NDPR grants Data Subjects[1] certain rights. In particular, a Data Subject has the right to (a) information, (b) data access, (c) data rectification, (d) data portability, (e) data erasure (also known as the right to be forgotten), (f) object to data processing, and (g) withdraw consent at any time.

To further its objectives, the NDPR mandates every person or organization that collects, uses, stores, or processes personal data to comply with certain obligations[2].

For instance, every Data Controller or Processor is required to:

i. carry out an audit of its data protection practices on or before 25 October 2019;

ii. display a privacy policy on every medium through which personal data is processed;

iii. appoint a 'Data Protection Officer', responsible for ensuring compliance with the NDPR; and

iv. establish a legal basis for data processing and data transfer to a foreign country or an international organisation.[3]

As part of its implementation mechanisms, Article 3.1.5 requires Data Controllers[4] to submit an initial audit report within six months of issuance of the Regulation, which lapsed on 25 July 2019. (Following appeals by industry players, this deadline was eventually extended for another three-month period, which elapsed on Friday 25 October 2019.[5]) Also, Article 3.1.7 requires Data Controllers who process the personal data of more than 2000 data subjects in a period of 12 months to submit, on

---

[1] The NDPR defines a "Data Subject" as an identifiable person; one who can be identified directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

[2] Depending on their specific dealings with data, these persons or organizations could either be Data Controllers or Data Administrators. Of course, the same person or organization could be a Data Controller **and** a Data Administrator if it determines the purposes for and the manner in which personal data is processed or is to be processed **and** actually does the processing. In this Paper, the term "Data Controller" is used throughout. Depending on the context, the term occasionally covers a "Data Administrator" also.

[3] See Part 4 of the NDPR.

[4] A Data Controller is a person who either alone, jointly with other persons 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.

[5] In November 2019, the Agency asked the licensed Data Protection Compliance Organizations to forward a list of companies who have audited their data protection practices before the October 25th deadline and communicated its readiness to sanction non-compliant organizations (Read more here: http://tribuneonlineng.com/data-protection-nitda-moves-to-sanction-defaulters-2/).

an annual basis, a summary of its data protection audit to the Agency, not later than the 15th of March of the following year.

Where the rights of a Data Subject under the NDPR is breached, the following penalties apply: 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; b) 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. These penalties are in addition to any other criminal liability.

The NDPR contains enforcement mechanisms that is somewhat different as those employed by other data protection regimes. The mechanisms entail the appointment of Data Protection Officers by every Data Controller for the purpose of ensuring adherence to the Regulation, the licensing of Data Protection Compliance Officers by the NITDA (the DPCOs will be engaged to conduct data protection compliance audit and consulting for Data Controllers), and the establishment of an administrative redress panel which investigate allegations of breach of the Regulations.[6]

Though considered 'revolutionary' in its own right, the NDPR has some flaws. For example, the Regulation does not contain provisions for privacy impact assessment, fails to adequately address the issue of data retention, and does not impose specific obligation to report data breach.

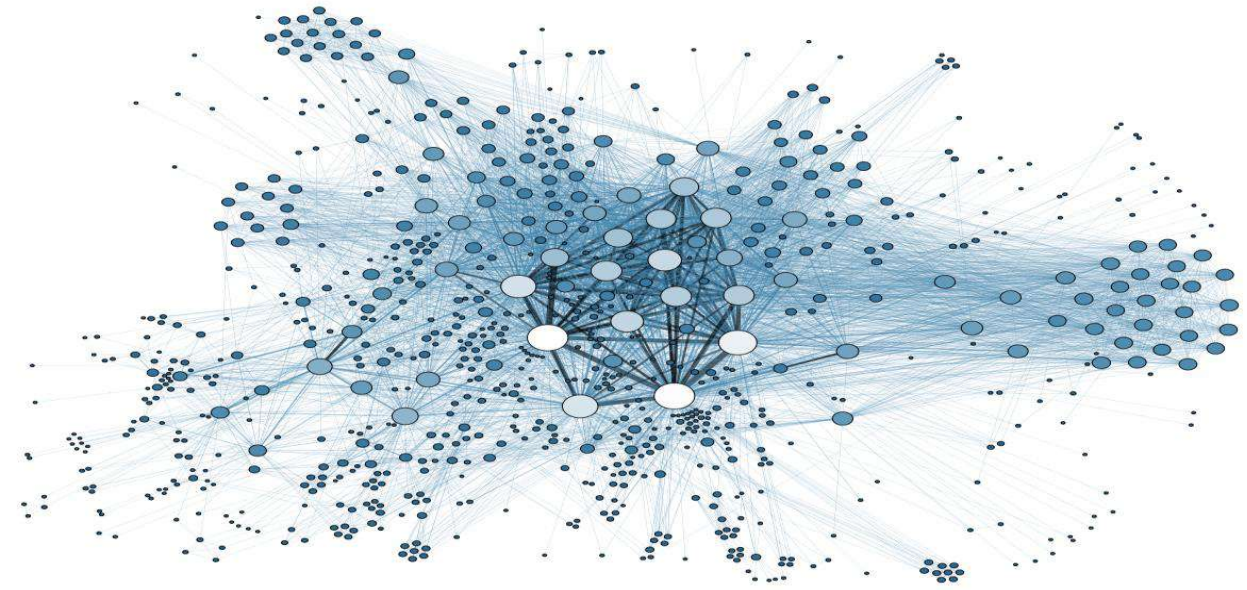
The NDPR also fails to provide any real protection for children by setting age limits to and in terms of parental consent requirements. In the United States, for instance, the processing of personal data of children below 13 years without parental consent is prohibited and this has been the law for more than two decades.

Also, under the European Union's General Data Protection Regulation, providers of information services are required to obtain parental consent before processing the personal data of children under 16 years of age.[7]

---

[6] Adekemi, Omotubura, 'The NITDA Regulations on Data Protection: A Peculiarly Nigerian Approach?' [NigerianLawToday, 2019] http://nigerianlawtoday.com/the-nitda-regulations-on-data-protection-a-peculiarly-nigerian-approach/ [accessed 10 February 2020]

[7] See Article 8 and Recital 38 of the General Data Protection Regulation (EU) 2016/679



General Legislation on Data Protection in Nigeria

a. *The Freedom of Information Act, 2011 (FoI Act):* Essentially made to promote transparency and open government, the FoI Act grants members of the public access to information held by (or on behalf of) public authorities. Section 14 of the Act, however, creates an exception by restricting public's access to information that contains personal information. But then, where a subject of an inquiry consents, or where a subject's personal information is publicly available, or where disclosure of personal information would be in the public interest, personal information may be disclosed.[8]

b. *The National Identity Management Commission Act 2007 (NIMC Act):* Section 26 of the NIMC Act restricts the access of any person or corporate body to the data or information contained in the database with respect to a registered individual entry without the authorisation of the Commission, except in certain, specified circumstances. The Act also makes it an offence for anyone to access data or information contained in the National Identity Database.

c. *Law Reform (Torts) Law, Ch. L82 Laws of Lagos State 2015*: Section 29 of the Law imposes a tortious liability on anyone who intentionally intrudes on the solitude or seclusion of another or private affairs, physically or otherwise, if the intrusion would be highly offensive to a reasonable person. Also, by the law, anyone who publicizes a matter concerning the private life of another is liable for invasion of

[8] See Section 14 (2) and (3) of the FOI Act

privacy, if the matter publicized is of a kind that: (a) would be highly offensive to a reasonable person and (b) is not of legitimate concern to the public.

d. *Constitution of the Federal Republic of Nigeria, 1999 (as amended) (CFRN):* Section 37 of the CFRN guarantees the protection of "the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications."[9] The right to privacy, as enshrined in the CFRN entails giving individuals the opportunity to control how and with whom, their data (or information) is shared, what data they choose to share, who can use their data, and for what purpose(s) their data can be used. Thus, privacy involves the means and techniques by which individual's data is protected from unlawful collection, use, manipulation, and storage. This is where data protection comes in.

e. *The Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (Cybercrimes Act):* Among other things, the Cybercrimes Act makes it an offence for anyone to unlawfully intercept personally identificable information such as computer and traffic data, mandates service providers to protect the individual's right to privacy under the CFRN and shall take appropriate measures to safeguard the confidentiality and integrity of data retained, processed or retrieved for the purpose of law enforcement.

f. *The Child's Right Act, 2003 (CRA):* Reenacting the spirit of the CFRN, Section 3 and 8 of the CRA protects the rights of a every child (persons under the age of 18) to privacy, family life, home, correspondence, telephone conversations, and telegraphic communications.

[9] See Section 37 of the Constitution of the Federal Republic of Nigeria, 1999 (as amended)

Sector-specific Legislation on Data Protection in Nigeria

a. *Nigerian Communications Commission (Registration of Telephone Subscribers) Regulations, 2011:* Section 9 of the Regulation mandates concerned entities to hold subscribers' personal information in strict confidence, to take reasonable precaution to maintain the integrity of personal information, and to utilise personal information collected only for specified purposes.

Section 10 of the Act prohibits the release of personal information to any security agent, licensee, or any other person, except where permitted by law. The Section also prohibits the release of subscribers' personal information to a third party and the transfer of subscribers' personal information, except with the consent of the subscriber and the NCC respectively.

b. *The Consumer Protection Framework for Banks and Other Financial Institutions Regulated by the Central Bank of Nigeria, 2016:* Enacted pursuant to the Central Bank of Nigeria Act 2007, the Framework prohibits financial institutions from disclosing customers' personal information. It also requires financial institutions to have appropriate data protection measures in place to prevent unauthorized 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.[10]

c. *The Central Bank of Nigeria Consumer Protection Regulations, 2019:* Issued in 2019 to improve compliance with the Consumer Protection Framework, the Regulations contain express provisions on data protection and privacy.

Among other things, the Regulations mandate every institution licensed and/or regulated by the Central Bank of Nigeria to protect the privacy and confidentiality of consumer information and assets against unauthorized access, obtain the written consent of consumers to collect and process their personal data for specific purpose and provide them with the option to withdraw the consent at any time, and inform consumers whenever their data is exchanged with an authorized third party, stating details of the exchange.

[10] See Paragraph 2.2.5 of the Framework

d. *The Central Bank of Nigeria Consumer Protection Guidelines on Responsible Business Conduct, 2019:* To promote god business practices, the Guidelines mandate financial institutions to protect the privacy and confidentiality of consumer information. The Guidelines define financial institutions broadly to include commercial banks, finance companies, payment service banks, payment terminal service providers, and other licensed providers of digital financial services.

e. *Guidelines for Nigerian Content Development in Information and Communication Technology (as amended, August 2019):* The relevant part of the Guidelines requires data and information management companies to host all sovereign data locally within the country and not outside the country, except with an express approval from NITDA.

f. *The National Health Act 2014 (NHA):* Under the NHA, health establishments are required to maintain health records for every user of health services and preserve the confidentiality of such records.[11] The NHA further imposes restrictions on the disclosure of user information, and requires persons in charge of health establishments to set up control measures for preventing unauthorized access to information.[12]

g. *The Consumer Code of Practice Regulations 2007 (NCC Code):* The NCC Code mandates telecommunication service providers to take reasonable steps to protect customer information against improper or accidental disclosure and to ensure that such information is securely stored. The NCC Code also restricts the transfer of customer information to any party, except as otherwise permitted or required by other applicable laws or regulations.[13]

h. *The Central Bank of Nigeria Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers, 2018 (Cybersecurity Framework):* Essentially, the Cybersecurity Framework outlines the minimum cybersecurity measures to be put in place by deposit money banks and payment service providers to ensure the confidentiality, integrity, and availability of data.

i. *The Credit Reporting Act, 2017 (The Act):* Section 9 of the Act protects data subject's right to privacy, confidentiality, and protection of their credit information.

---

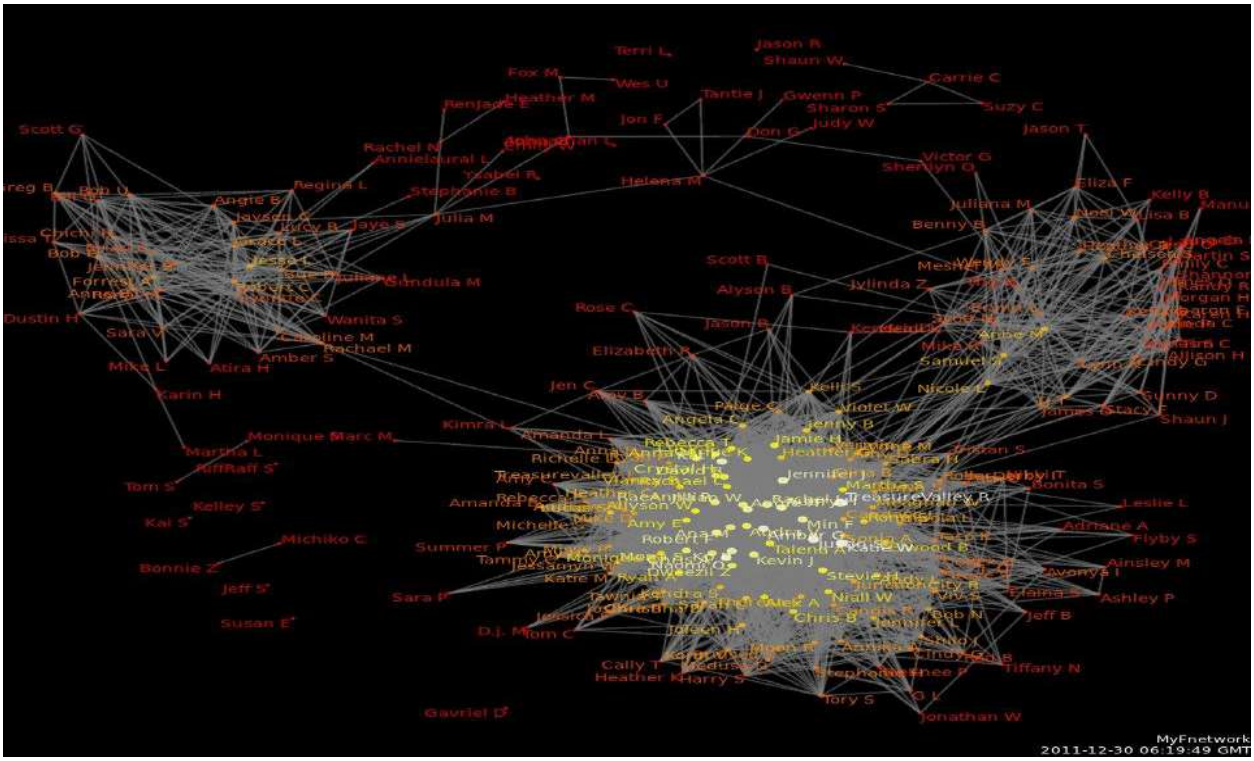
[11] See Section 25 of the NHA
[12] See Section 29 of the NHA
[13] See Item 35 of the Schedule to the Consumer Code of Practice Regulations, 2007

Proposed Legislation on Data Protection in Nigeria

In rounding off this part, it is essential to note that there are two legislation, which when passed, are expected to further bolster the data protection regime in Nigeria:

a. *Draft Nigeria Data Protection Regulation 2019 – Implementation Framework (Draft NDPR Framework):* In July 2019, NITDA published its draft NDPR Framework and sought the contributions of stakeholders. The Framework clarifies the provisions of the NDPR and contains useful templates.

b. *Nigerian Data Protection Bill:* Awaiting the President's assent, the Bill seeks to, among other things, establish a Data Protection Commission – a supervisory authority that would protect the privacy of personal data.



The Importance of an Adequate Data Protection Regime

At the core of data protection legislation is the ambition to protect individual's right to informational privacy and secure lives and property—this is achieved through a series of measures designed to curb unauthorized access to or disclosure of personal information and incidences of cyberbreach in a growing (and progressively volatile) data environment.

Asides this, data protection legislation provides a legal basis for challenging excessive collection and unlawful use of data, negligent data handling, incorrect documentation of sensitive information, and growing corporate and state-sponsored surveillance activities.

Now that the dominant business model requires maximum data collection, behavior tracking, and fostering of addiction, many countries are making efforts to safeguards the value of citizens' personal data, and so most data protection regimes now identify a white list of countries—that is, countries with basic data protection law and which affords Data Subjects the privilege to enforce their rights, either in such country or in the international courts. An adequate data protection regime guarantees an inclusion in this white list and essentially eases the inbound transfer of data, which is essential for virtually every form of trade powered by technology.

In terms of economic implications, the existence of a certain data protection regime fosters the integrity and growth of commerce, generally improves the ease of doing business. and forms the backbone of a thriving digital economy: without it, it would be practically impossible to conduct economic activities in a world where data is fast becoming the most valuable economic resource.

On a related note, a data protection regime also provides businesses with the opportunity to improve brand perception by turning respect for personal information into competitive differentiators.

Ademola Adeyoju
Intellectual Property & Technology Lawyer
Email: ademolaadeyoju1@gmail.com
Phone: +234-8136593482