Privacy and Data Protection
4th July 2019.


Yimika Ketiku[1] **Dolapo Bolu**[2]

DATA PROTECTION REGULATION 2019: THE NEW LAW

1. INTRODUCTION

A more centralized data security and privacy law has emerged in Nigeria with the passing of the Nigeria Data Protection Regulation 2019 ("the Regulation") by the Nigerian Information Technology Development Agency ("NITDA").

With many public and private bodies migrating their respective businesses and other information systems online, information solutions in both the private and public sectors now drive service delivery in the country through digital systems.[3]

This paper provides an overview of data privacy and protection in Nigeria with a specific focus on the Nigeria Data Protection Regulation 2019.

2. DATA PRIVACY AND PROTECTION IN NIGERIA

In this new digital age and with data being referred to as "the new oil", data has become highly valuable and data privacy and protection has come to the forefront. Many countries are now taking steps to ensure that the data and privacy of their citizens are adequately protected. In May 2018, the European Union released the General Data Protection Regulation (GDPR) to deal with data protection and violations stemming from it. The GDPR has revolutionized the way data protection and privacy is viewed. The Regulation mirrors the GDPR because it makes businesses or organizations liable if they or their third-party contractors handle

[1] Senior Associate, Corporate Finance & Capital Markets, SPA Ajibade & Co., Lagos, NIGERIA.
[2] Associate, Corporate Finance & Capital Market, SPA Ajibade & Co., Lagos, NIGERIA.
[3] Preamble of the Nigeria Data Protection Regulation 2019.

citizens' or residents' personal data without complying with the privacy laws. Hopefully, the Regulation will promote increased foreign investment and opportunities for Nigerians.

Inspite of the rapid growth of technology and digitization in Nigeria, there has been no comprehensive legislation that set out to protect the data of Nigerian citizens. Section 37 of the Constitution[4] provides that "…the privacy of citizens, their homes, correspondence, telephone conversations, and telegraphic communications is hereby guaranteed and protected…" and some sector-specific data protection regulations such as the NCC[5] Consumer Code of Practice Regulations and the Consumer Protection Framework of the CBN[6] seek to protect the handling and transferring of data.

The National Information Technology Development Agency ("the Agency") is the primary regulatory authority responsible for the administration of electronic governance and monitoring of the use of electronic data and other forms of electronic communication transactions in Nigeria. Section 6 of the National Information Technology Development Agency Act ("NITDA Act")[7] sets out the mandate of the Agency. It stipulates that:

"*The Agency shall-*

(a) Create a framework for the planning, research, development, standardization, application, coordination, monitoring, evaluation and regulation of Information Technology practices, activities and systems in Nigeria and all matters related thereto.

(b) Provide guidelines to facilitate the establishment and maintenance of appropriate [sic] for information technology and systems application and development in Nigeria for public and private sectors, urban-rural development, the economy, and the government;

(c) Develop guidelines for electronic governance and monitor the use of electronic data interchange and other forms of electronic communication transactions as an alternative to paper-based

[4] Constitution of the Federal Republic of Nigeria 1999.

[5] NCC Consumer Code of Practice Regulations, 2007.

[6] Consumer Protection Framework of the Central Bank of Nigeria, 2016 https://www.cbn.gov.ng/out/2016/cfpd/consumer%20protection%20framework%20(final).pdf.

[7] Act No. 28 of 2007 (published in Official Government Gazette No. 90 Vol. 94, 5th October 2007).

methods in government, commerce, education, the private and public sectors, labour, and other fields, where the use of electronic communication may improve the exchange of data and information."

The Agency issued the Regulation on 25th January 2019. The Regulation sets out to deal comprehensively with the protection of the personal information of Nigerian citizens and anyone resident in Nigeria. An understanding of its contents is crucial to appreciating how far companies can go when handling personal data.

Data is an important and key aspect of the operations of digital organizations and many other businesses. The provisions of the Regulation are stringent and have been enforceable since its issuance, therefore companies and organizations that handle data must take them into cognizance in their dealings going forward.

3. HIGHLIGHTS

3.1 Application: The Regulation applies to all residents of Nigeria, all citizens of Nigeria residing outside of Nigeria and all organizations processing personal data of such individuals. It seeks to protect the privacy of individuals by setting standards for the collection, processing, storage, usage, and disclosure of personal data by organizations in a manner that is not prejudicial to the dignity of a human person.

The Regulation applies to *"all transactions intended for the processing of personal data, to the processing of personal data notwithstanding the means by which the data processing is being conducted or intended to be conducted in respect of natural persons in Nigeria"*[8] In summary, the Regulation applies to private and public organizations, including not-for-profit.

The Regulation defines the "Data Administrator as a person or an organization that processes data.[9] "Data Controller" is defined as a person who either alone, jointly with other persons or in common with other persons or a statutory body determines the purposes for or the manner in which personal data is processed or is to be processed.[10]

3.2 Data Processing Principles: Personal data shall be:

(a) **"***Collected and processed in accordance with specific, legitimate and lawful purpose consented to by the Data Subject;*

[8] NDPR, at Art. 1.2 (a).

[9] Ibid at Art. 1.3(ix).

[10] Ibid at Art. 1.3(x).

(b) Adequate, accurate and without prejudice to the dignity of the human person;

(c) Stored only for a period within which it is reasonably needed; and

(d) *Secure against all foreseeable hazards and such as theft, cyberattack, viral attack dissemination, manipulation of any kind, damage by rain, fire and exposure to other natural elements*."[11]

Lawful processing of personal data requires (1) consent of the data subject; (2) for the performance of a contract; (3) for compliance of a legal obligation; (4) to protect the vital interests of the data subject; and (5) for the performance of a task carried out in the public interest.[12]

The Regulation stipulates that organizations are responsible for the personal data that is in their custody or control. Organizations owe a duty of care to the Data Subject and also are accountable for all acts and omissions of data processing.[13]

3.3 Third-Party Contracts: A Data Controller shall enter into a written contract with any third-party processing data on its behalf. In addition, if an organization engages a third party to handle personal data collected by the organization, the organization is also responsible for the third party's compliance with the Regulation.[14]

Organizations can contract with service providers, including cloud computing service providers to process and store client and employee personal information. The service providers can be located outside Nigeria. However, if an organization does use a foreign service provider, the processing shall be subject to the Regulation and supervision of the Honourable Attorney General of the Federation ("HAGF").[15]

In addition, the organization must include in its policy the access (if any) of third parties to personal data and purpose of access.

An organization which transfers the processing of personal data to a foreign country or an international organization shall ensure the following systems are in place:

3.3.1 an adequate level of protection;

3.3.2 privacy protection oriented legal system of the foreign country;

3.3.3 implementation data protection rules;

[11] Ibid Art. 2.1(1)(a – d).
[12] Ibid at Art. 2.2 (a-e).
[13] Ibid at Art. 2.1 (2 & 3).
[14] Ibid at Art. 2.7.
[15] Ibid at reg. 2.11.

3.3.4 the existence and effective functioning of one or more independent supervisory authorities; and

3.3.5 the international commitments form legally binding conventions or instruments.[16]

For example; if an organization decides to use a cloud computing service provider located in the United States, that organization should be aware of the Patriot Act.[17] The Patriot Act allows the United States government to intercept and access electronic communications and business records. Any data stored in United States data centers, regardless of ownership, fall under United States law, including the Patriot Act.

3.4 **Privacy Policy:** Organizations must display a "simple and conspicuous" and easily understandable privacy policy that contains specified content. The Regulation requires the organizations to develop and follow privacy policies that are reasonable and as stipulated under regulation 2.5 (a–i), so that the organization meets its obligations under the Regulation.

3.5 **Consent:** There are specific requirements for obtaining consent. This is an important and crucial requirement of the Regulation. Section 2.1 of the Regulation stipulates that the "data subject" who is generally any identifiable person, must consent before any data is collected and that personal data must be collected and processed in a lawful manner. Organizations may only collect, process and disclose personal data for purposes that are reasonable and only to the extent that it is reasonable for meeting the purposes for which the information was collected.[18] Data Controllers may also only process the collected personal information for the purposes for which the information was originally collected.[19] When a Data Controller collects personal data from a Data Subject, it must give that individual notice of the purpose of collection. It is also advisable that the Data Subject is provided with the contact of the personnel within the organization that can answer any questions regarding the personal data collected.

[16] Ibid Art 2.11 (a – e).

[17] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub L No 107-56, 115 Sta 272 (2001).

[18] Ibid at reg. 2.2.

[19] Ibid at reg. 2.3.

3.6 **Data Security:** Article 2.1(d) of the Regulation stipulates that personal data shall be:

"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".

The breach of data security amounts to a loss of privacy. Hence, Article 2.6 stipulates measures to protect personal data. The Data Controller is to ensure the security of personal data collected. We would advise that the Data Controller should establish security measures that reflect the sensitivity of the personal data it collects and handles. Highly sensitive personal data would require the most security, while anonymous data would require the least amount of protection.

Individuals that suffer loss of privacy may use the Regulation to initiate proceedings against organizations that disclose personal information without authorization due to a security breach.

However, the Regulation does not provide a procedure to follow where there is a breach. One would expect that an organization that suffers a security breach would notify the NITDA of an incident that involves the loss of, unauthorized access to, or disclosure of personal data that may pose a real risk of significant harm to individuals. The organization should also notify the affected individuals and organizations may do so under their own initiative. Furthermore, it is advisable for organizations to notify data subjects of available remedies in the event of a breach of their privacy policy and the time frame for the remedy.

3.7 **Implementation:** The Regulation sets out specific provisions for implementation for both public and private organizations and they include the following:

- All organizations that control personal data shall within 3 months of the issuance of the Regulation, release to the public their data protection policies, which shall conform with these Regulations;[20]
- There shall be a Data Protection Officer, to ensure compliance with the Regulations;[21]
- Within 6 months after the date of issuance of the Regulations, an Organization must conduct an audit of its privacy and data protection services;[22]

[20] Ibid at reg.4.1(1).
[21] Ibid at reg. 4.1(2).
[22] Ibid at reg. 4.1(5).

- Where a Data Controller processes the personal data of more than 1000 data subjects in a period of 6 months, it shall submit a soft copy of the summary of the audit to the Agency;[23]
- Where a Data Controller processes the personal data of more than 2000 Data Subjects in a period of 12 months, it shall submit a summary of its data protection audit to the Agency.[24]

3.8 Penalties for Default: Any person who is subject to the Regulation, who is found to be in breach shall be liable to the following:

- A Data Controller dealing with more than 10,000 Data Subjects, shall be subject to the payment of a fine of 2% of its Annual Gross Revenue of the preceding year or payment of the sum of ₦10,000,000 [ten million Naira], whichever is greater;
- A Data Controller dealing with less than 10,000 Data Subjects, shall be subject to the payment of the fine of 1% of the Annual Gross Revenue of its preceding year or payment of the sum of ₦2,000,000 [two million Naira], whichever is greater.[25]

4. CONCLUSION

The standards set out in the Regulation are reasonable. The Regulation imposes clear obligations on organizations. Hence, an organization that collects personal data should ensure that:

a. Personal data collected can only be used for the required purpose and no other purpose;

b. Personal data collected is held "in trust" for the Data Subject's benefit;

c. There is no disclosure of personal data without consent;

d. It implements safeguards to protect personal data; and

e. Service providers destroy or return all personal data collected and processed at the end of the contract.

[23] Ibid at reg. 4.1(6).
[24] Ibid at reg.4.1(7).
[25] Ibid at reg 2.10(a – b).

This Regulation ensures that the protection of personal data in Nigeria is in consonance with developing global best practices and fills the gap in the regulation of privacy rights and data protection in Nigeria, in the absence of a comprehensive legislation from the National Assembly.[26]

For further information on this article and area of law, please contact
Yimika Ketiku or Dolapo Bolu at S. P. A. Ajibade & Co., Lagos
by telephone (+234 1 472 9890), fax (+234 1 4605092)
Mobile (+234.809.990.0344) or (+234.08150865646)
Email: yketiku@spaajibade.com or dbolu@spaajibade.com
www.spaajibade.com

[26] See the proposed Data Protection Bill [HB02] 2019 passed by the legislative Houses, but which failed to receive the Presidential assent in June prior to the dissolution of the Eighth Assembly.