OMAPLEX LAW FIRM
(O.M. Atoyebi, SAN & Partners)

IS AFRICA'S DATA PROTECTION IN CRISIS? THE NIGERIAN EXPERIENCE

Introduction

On the 15th of January, 2019, the Nigerian government issued the Nigerian Data Protection Regulations[1], marking the Nation's first attempt at having a comprehensive legislation on data protection. The reactions trailing its passage have been a mixed bag: whist the regulations have been loudly applauded in some quarters as the right step towards achieving national data protection, others believe that it is of no positive consequence as it merely adds to a long list of government legislations and regulations that are rarely enforced for want of the political will to do so.

Data Protection, the Nigerian Experience

Perusing through the contents of the 5-paged regulation, governing Data Protection in Nigeria, one can understand the optimism of those that believe in the prospects of the Regulations in the light of salient notable provisions contained therein.

First, the Regulation articulates the privacy rights of Nigerian citizens enshrined in **Section 37** of the **Constitution** of the **Federal Republic of Nigeria, 1999 (as amended)**.

In the wake of the passage of the NDPR, the Federal High Court sitting in Abuja, in **Incorporated Trustees of Paradigm Initiative for Information Technology (PIIT) & Sarah Solomon-Eseh v. National Identity Management Commission (NIMC) & Anor[2]**, reaffirmed the privacy rights of Nigerians as it ordered the Nigerian Information Management Commission to implement adequate steps to safeguard the privacy rights of Nigerian citizens beyond merely having spurious security policies which it had prior to the suit, and it failed to implement.

In another welcome development, the NDPR raises the standard of the duty of care expected of Data Controllers by mandating all such Data Controllers to take steps to curb cybercrimes and like threats involving data rights infringement by employing data encryption technologies, developing organizational policy for handling personal data, the protection of emailing systems amongst others.[3]

With the decision of Fintech giants *Paypal*, to restrict foreign payments into Nigeria owing to the prevalence of advanced fee frauds (*Yahoo-Yahoo*) in the country[4], the issuance of a regulation as the NDPR which creates a sense of a protection culture must be applauded albeit with reservations as to the efficacy of its enforcement or the adequacy of its provisions to ensure a stellar data protection status in Nigeria.

Moving away from the laudable data security benefits offered by the NDPR to the Nigeria populace, from an economic standpoint, it is indeed to the credit of the NDPR, that it has created a revenue generation avenue for the Federal Government. Articulating the economic

[1] NDPR, 2019
[2] Andersen Tax Lp, Federal High Court Affirms The Data Privacy Rights of Nigerian Citizens' <https://www.mondaq.com/nigeria/privacy-protection/841960/federal-high-court-affirms-the-data-privacy-rights-of-nigerian-citizens> accessed September 3, 2020.
Premium Times, 'The Huge Prospects of Nigeria's Data Protection Regulation 2019, By Isa Ali Ibrahim Pantami' (*Premium Times,* 16 April 2019) accessed 7 September 2020.

[3] NDPR Art. 2.6, 2019.
[4] Jacob Mugendi, 'The Societal Cost of Cybercrimes' (*iAfrikan* 21st May 2020) < https://www.iafrikan.com/2020/05/21/crime-punishment-africa-cybercrime-nigeria-kenya-yahoo-yahoo/ > accessed September 3, 2020.

potential of the NDPR, Isa Pantami, Nigeria's Minister of Communications and Digital Economy observes succinctly:

> "One of my greatest sources of joy on the Regulation is its job creation potential. Over 1.5 million businesses and non-governmental organisations would need to file Data Audit Reports on or before March 15 every year. Each of these reports must bear a Verification Statement, sign and seal of a licensed DPCO. If each DPCO provides service for an average of 50 Data Controllers, we would need over 300,000 professionals to meet this need."[5]

Whilst the provisions of the NDPR are commendable, as they set Nigeria on the path to achieving a stellar data protection status, conundrums abound in many aspects. The poor level of compliance with the provisions of the NDPR is perhaps the biggest bane in achieving data protection in Nigeria. Available reports show that at the close of the year in 2019, only 94 companies had submitted their data audit reports to the National Information Technology Development Agency (NITDA). Although the NDPR requires only organizations processing data of up to 2,000 subjects to file reports, in a nation as large as Nigeria with several thousand bank branches scattered across the country, 160 universities and at least 23,640 public and private hospitals, 94 data audit reports are a far cry from compliance.[6]

The NITDA is nonetheless also complicit in the poor level of compliance recorded in the country. Having implicitly set July 25th 2019 as the deadline for filing data audit reports, the late release of a list of licensed DPCOs in 2019, made compliance almost impossible. This delay ultimately culminated in the agency granting a 3-month extension for compliance. Despite the extension, it remains clear that the 94 occasions of compliance in the reports recorded show that Data Controllers in the country like the NITDA were all but prudent about ensuring data compliance in the country.

The high costs associated with compliance is also contributory to the delays in achieving the highly desired data protection compliant status. Engaging the services of diligent top tier firms in Nigeria for data auditing purposes costs as much as N2,500,000. Such prices, with the reality of economic hardships in Nigeria would see several companies unable to afford the costs of data compliance.

Moving on, another problem observable are the security provisions of the NDPR on data which to the less keen eye would seem fool proof. First, although data processors are mandated to inform the NITDA of data breaches, they are not obligated to inform persons whose data have been so breached. This problem is put into perspective, where the data obtained could potentially be a tool in harming a data subject. Shouldn't a public body like the National Identity Management Commission (NIMC) which controls data of basically the entire blueprints of the lives of several Nigeria be mandated to inform Nigerians of a breach in its data base? In sharp contrast, **Article 34** of the **General Data Protection Regulation (GDPR)**[7] mandates data controllers to promptly inform data subjects of such breaches.

The narrow definition of data under the NDPR is also a cause for concern. In its very limited definition of data, the concept is defined to only capture electronic data.[8] This raises the question as to whether data stored in non-electronic forms are not afforded the protections guaranteed under the NDPR? This is indeed a cause for worry as several government institutions within the country still rely heavily on traditional methods of data storage and processing.

The 60-day deadline issued by the NITDA for all public institutions to digitize their databases elapsed long ago in July 2020[9]. Nothing more has been heard in this regard as public offices still operate at the status quo.

Perhaps it can be argued that where a suit bothering on whether the NDPR extends to non-electronic data arises, the courts by judicial activism would so interpret the NDPR to extend to traditional data. But it is feared that such might not be the case considering the instance of several opposing/contradicting Supreme Court judgements on the admissibility of computer-generated evidence prior to the passage of the Evidence Act of 2011.

The Path Towards Reforming Data Protection in Nigeria

Rome was certainly not built in a day and similarly, Nigeria's quest to achieving a compliant data protection status has only begun. Nonetheless, the above issues discussed are cardinal and must be tackled. In doing so, it is germane that the NITDA as the principal body for data protection in Nigeria, step up. Whilst the agency must be applauded for opening investigations into a number of alleged data breaches, notably breaches by TrueCaller,

[5] Premium Times, 'The Huge Prospects of Nigeria's Data Protection Regulation 2019, By Isa Ali Ibrahim Pantami' (*Premium Times,* 16 April 2019) accessed 7 September 2020.

[6] Adekunbi Ademola, ' How Safe is Your Data' (*StearsBusiness* 22 May 2020) < https://www.stearsng.com/article/how-safe-is-your-data> accessed 5 September, 2020.

[7] GDPR, 2016.

[8] NDPR, Art. 1.3(iv), 2019.

[9] Ruth Okwumbu, 'Public Institutions to Digitize Database in 60 days, NITDA orders' (*Nairametrics,* 18 May 2020) <https://nairametrics.com/2020/05/18/public-institutions-to-digitize-databases-in-60-days-nitda-orders/#:~:text=The%20National%20Information%20Technology%20Development,to%20securely%20digitize%20all%20databases. > accessed 7 September, 2020.

Surebet247 and the Lagos Inland Revenue Service, the lack of sanctions or the failure to publicize same raises concerns that the agency is a toothless bulldog.

The agency must begin to impose sanctions on defaulting organisations. The NITDA should take a cue from countries within the European Union which have imposed €114,000,000 in fines since the inception of the GDPR in 2016[10].

In a similar vein, government agencies which account for a majority of data controllers processing data of millions of Nigerians must desist from the continued lackadaisical attitude shown towards data compliance in Nigeria. In the wake of the Covid-19 pandemic, it is without doubt that data of millions of Nigerians have been processed for possible tracking and monitoring of Covid-19 patients and their contacts. But it is rather worrying that on the official website of the Nigerian Centre for Disease Control (NCDC) there exists no privacy policy popping up to indicate that measures are in place to protect the data of millions of Nigerians being processed and the narrative is same for big data processors like the NIMC, the Joint Admission and Matriculation Board and the Corporate Affairs Commission.

The definition of data under the NDPR must be reviewed to explicitly include non-electronic data. This is in tandem with the reality that several public institutions in Nigeria continue to rely on traditional methods of recording data. An amendment in the NDPR in this regard is needed to avoid the unwanted scenarios that may so arise as earlier stated.

Such an amendment must also include an obligation on data controllers to inform data subjects of data breaches thus affording such subjects the opportunity to take extra precautionary measures and further ultimately bring the NDPR into conformity with international best practices on data protection.

Lastly, it is firmly believed that by licensing more competent Data Compliance Officers, market forces would operate to dictate cost of data audit reports and associated due diligence on data compliance. This would remedy the effect of the current regime were high compliance costs currently cripple the efforts of Data Controllers on achieving compliance.

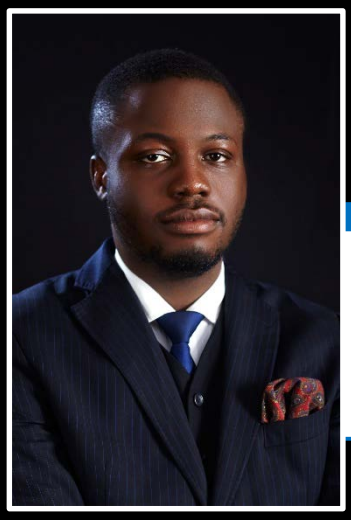
Conclusion

Undoubtedly, in the light of the realities of the Covid-19 era, there is now more than ever, the need to boost the oversight functions in ensuring data compliance more so, in an age of unprecedented reliance on data by private individuals and entities as well as governments of nations, in making pragmatic decisions. It is without doubt, that the Nigerian government must step up efforts to meet global best practices on data protection and compliance.

[10] Dereek Preez, 'The Impact of GDPR - 160,000 Breach Notifications in Europe and €114m in Fines' (*Diginomica,* 21 January 2020) accessed September 11, 2020.

OMAPLEX LAW FIRM
(O.M. Aloyebi, SAN & Partners)

Author



Echoga Caleb

caleb.echoga@omaplex.com.ng