Nigeria's data protection legal and institutional model: an overview

Nigeria's data protection legal and institutional model: an overview

Olumide Babalola*

Key Points

- In the past two decades, the unprecedented incursion of technology into the economic and socio-cultural activities in Nigeria increasingly posed many unanswered questions on data protection and privacy. Consequently, this led to the country's numerous attempts to enact a principal data protection legislation in addition to the existing sectoral laws on the subject.
- Despite its ratification of the Economic Community of West African States (ECOWAS) Supplementary Act on data protection in 2010, Nigeria carried on without a general data protection legislation until nine years later when the National Information Technology Development Agency (NITDA), in a face-saving regulatory move, issued the Nigeria Data Protection Regulation (NDPR) as Nigeria's first all-encompassing and comprehensive, albeit subsidiary legislation on data protection.
- This article provides an analytical synopsis of Nigeria's current legal framework on data protection touching its brief history, the general and sectoral enactments on data protection, the enforcement mechanism created under the NDPR as well as the Implementation Framework issued in the mould of guidance notes.

Introduction

Nigeria has had subsidiary data protection legislation for over two years but its legal framework around the subject lacks holistic academic appraisal to date. The Nigeria Data Protection Regulation[1] (NDPR) which remains the country's most comprehensive piece of (subsidiary) legislation on data protection substantially mirrors the EU General Data Protection Regulation (GDPR) in its scope, definitions of terms, principles of data processing and enforcement mechanism albeit not without its own teething problems.[2] Being the 25th country to regulate data protection in Africa,[3] expectations are unsurprisingly high on Nigeria's model of redress and enforcement mechanisms, however, little academic attention has be devoted to the NPDR 'classic' particularly in relation to the data protection ecosystem in Nigeria.

This article is divided into four main sections: the first briefly gives a background of data protection in Nigeria by capturing the legislative and administrative trajectory enroute the issuance of NDPR[4] while the next section focuses on Nigeria's legal and regulatory regime on data protection by introducing the relevant international instruments and municipal statutory provisions under the general and sector-specific enactments duly passed by the parliament or released by public bodies during the pre- and post-NDPR issuance. The third section is an examination of the enforcement mechanisms and the major actors in the country's data protection ecosystem with an emphasis on the National Information Technology Development Agency (NITDA) as Nigeria's data protection authority[5] (DPA) and its licenced agents. This is done by examining some regulatory

*Olumide Babalola, School of Law, University of Reading, UK; Barrister and Solicitor of the Supreme Court of Nigeria; Managing Partner, Olumide Babalola LP,. Email: Nigeria counsel@oblp.org

1 NDPR was released by the National Information Technology Development Agency (NITDA) on the 25th day of January 2019. Although, a subsidiary legislation, it is Nigeria's only enactment wholly dedicated to data protection.

2 Graham Greenleaf, 'Nigeria Regulates Data Privacy: African and Global Significance' (2019) 158 Privacy Laws & Business International Report (2019) 23 UNSWLRS 66.

3 Nigeria comes behind Cape Verde (2001), Burkina Faso, Tunisia, Mauritius (2004), Senegal (2008), Benin, Morocco (2009), Angola, Gabon, Lesotho (2011), Ghana (2012), Cote d'Ivoire, Mali, South Africa (2013), Chad, Madagascar (2015), Equatorial Guinea, Guinea Conakry, Malawi, Mauritania (2016), Niger (2017), Algeria, Botswana, and Kenya (2018).

4 Here, this article deliberately underplays the nexus between privacy and data protection so as to avoid any conflation in the history of the closely linked concepts.

5 In this article, the term DPA is used interchangeably with supervisory authority (SA).

responsibilities imposed on data controllers in the light of administrative sanctions for default as well as NITDA's legitimacy issues. The article concludes in the fifth section with a recap of the issues discussed and closing observations.

History of data protection in Nigeria

While some Nigerian academics have argued that privacy extends to data protection and should not be estranged from the former,[6] the other proponents have argued that data protection should be completely severed from privacy.[7] However, until the Nigerian appellate courts specifically bifurcates data protection from privacy, the history of data protection will continue to be linked to constitutional developments in Nigeria. Notwithstanding the relation of both concepts, this article focuses squarely on data protection with minimal reference to privacy even though all existing schools of thought on the subject agree data protection originated from privacy.

The concept of data protection in Nigeria owes its origins to the incursion of technology in the country's economic activities when the erstwhile communal standard of living characteristic of the Nigerian societies, like their African counterpart, had given way to the realization of the importance to protect personal information from untoward use, at a time when the importance of (personal) data to most businesses had become more intrinsically pronounced.[8]

Data protection in Nigeria has a checkered history, one plagued with little or no documentation, failed legislative attempts, judicial indifference, and political mind games etc. The first legislative attempt at regulating data protection was the Computer Security and Critical Information Infrastructure Protection Bill 2005, but the objectives of the abortive bill revealed it was substantially meant to criminalize 'illegal conducts against ICT systems' and cybercrime.[9] While a negligible clause masqueraded as a provision on consent and purpose limitation, the bill's ultimate aim was to prosecute offenders rather than provide remedies to victims of data breaches.[10] After its first unsuccessful legislative appearance in 2005, the bill resurfaced in 2011 but was withdrawn before completing its legislative cycle.[11]

The next verifiable legislative attempt was made in October 2008 when the Nigerian government, in the company of other African states, initiated moves towards the eventual adoption of the Supplementary Act on personal data protection within the Economic Community of West African States (ECOWAS Act)[12] at the 37th session of the authority of Heads of State and Government in Abuja on the 16th day of February 2010.[13] By that international treaty signed by former President Goodluck Jonathan, Nigeria's undertaking to 'establish a legal framework of protection for privacy relating to collection, processing, transmission, storage and use of personal data . . . ' remotely culminated in the Data Protection Bill 2010 targeted at 'reducing' unauthorized processing and use of personal data and information without the prior consent of the data subjects.[14] The bill was reputed to be the first federal legislative proposal wholly

6 Within the Nigerian context, the right to privacy is guaranteed by section 37 of the Nigerian 1999 Constitution as 'privacy of citizens' and this phrase is expansive enough to accommodate all types of privacy especially since the wording of the Constitution does not qualify, limit or restrict its meaning to exclude information privacy which embodies data provision. The Nigerian Constitution also guarantees privacy of correspondence, telephone conversations and telegraphic communications which are fused with information privacy. See France Belanger and Robert E Crossler, 'Privacy in Digital Age: A Review of Information Privacy Research in Information Systems' (2011) 35(4) MISQ 1017–41. To demonstrate the elasticity of 'privacy of citizens', the Nigerian Court of Appeal notes that the phrase is wide enough to protect a citizen's body, life, person, thought, conscience, belief, desires, health, relationship, character, possession, family and all aspects of his life. See *Nwali v Ebonyi State Independent Electoral Commission* (2014) LPELR 3682 (CA).

7 Adekemi Omotubora and Subhajit Basu, 'Next Generation Privacy' (2020) 29(2) Information & Communications Technology Law 151–73; Lukman A Abdulrauf and Charles M Fombad, 'Personal Data Protection in Nigeria: Reflections on Opportunities, Options and Challenges to Legal Reforms' (2016) 38(2) Liverpool Law Review 1; Andrew U Iwobi, 'Stumbling Uncertainly into the Digital Age: Nigeria's Futile Attempts to Devise a Credible Data Protection Regime' (2016) 26(3) Transnational Law and Contemporary Problems 13; Yinka Olomojobi, 'Right to Privacy in Nigeria' (2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3062603> accessed 17 March 2020; Enyinna Sodienye Nwauche, 'The Right to Privacy in Nigeria' (2007) 1(1) CLAS Review of Nigerian Law and Practice 66–90; Iheanyi Samuel Nwankwo, 'Information Privacy in Nigeria' in Alex B Makulilo (ed), *African Data Privacy Laws* (Springer International Publishing, Switzerland, 2018) 45.

8 Alex B Makulilo, 'The Quest for Information Privacy in Africa' (2018) 8 Journal of Information Policy 317.

9 Bernard O Jemilohun and Timothy I Akomolede, 'Regulations or Legislation for Data Protection in Nigeria? A Call for a Clear Legislative Framework' (2015) 3(4) Global Journal of Politics and Law Research, 1–16.

10 Ibrahim Yusuff, 'A Critical Review of the Computer Security and Critical Information Infrastructure Protection Bill 2005 as Nigerian Specific Cybercrime Legislation' (2015) <https://martinslibrary.blogspot.com/2015/03/a-critical-review-of-computer-security.html> accessed 9 March 2021.

11 See Uchenna Jerome Orji, *Cyber Security Law and Regulations* (1st edn, Wolf Legal Publishers, Nijmegen, The Netherlands, 2012) 151.

12 A/SA.1/01/10 adopted in Abuja on the 16th day of February 2010.

13 Abdullahi M Abdulquadir, 'Regional Trade and the Challenges of Data Protection in West Africa' (2020) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3770159> accessed 17 February 2021.

14 Abubakar S Aliyu, 'The Nigerian Data Protection Bill: Appraisal, Issues and Challenges'
(2016) 9(1) The Innovative Issues and Approaches in Social Sciences Journal 48.

focused on data protection but after scaling the first reading, nothing was recorded or heard of the bill again.

A year later, the Data Protection Bill 2011 was again sponsored to the National Assembly, but the poorly drafted and comparatively weak document did not unsurprisingly get to the President for his assent.[15] In 2015, another bill styled Data Protection Bill 2015 was passed by the Federal House of Representatives, but it was either renamed or unsuccessful at Senate.

Again in 2016, the National Identity Management Commission proposed the Personal Information and Data Protection Bill with provisions on the collection use and disclosure of personal information and sponsored same to the House of Representatives, but it did not pass legislative scrutiny. In 2017, the Speaker of House of Representatives sponsored another Data Protection bill which also never crossed the legislative hurdles.

In 2018, before the issuance of the NDPR, the Council of Europe in conjunction with the Federal Ministry of Justice and some other stakeholders drafted the Nigerian Data Protection Bill 2018 and it was finally passed into law in 2019 but unfortunately, the President withheld his assent thereby plunging the country back to square one.[16] Worthy of note is also the 2013 (draft) Guidelines on Data Protection issued by the NITDA but was never released.[17] Ultimately, in 2020, the Nigerian government proposed another draft Data Protection Bill 2020 and invited the public to make comments at a validation workshop held in September 2020 but nothing has been heard about bill ever since.

The foregoing chronicle shows the many failed attempts by the Nigerian State to enact a principal data protection law long before the makeshift issuance of the NDPR which is fraught with many questions, including NITDA's legitimacy to regulate data protection, NDPR's force of law as a subsidiary legislation, its untidy adoption of both American and European concepts, omission of legitimate interest as a basis of lawful processing etc—which issues can only be cured by a principal legislation.

Legal and regulatory regime of data protection in Nigeria

Data protection in Nigeria is regulated or influenced by a number of principal and subsidiary legislation. While it is conceded that data protection is not generally regulated by a principal Act, many relevant international and municipal laws make various provisions bordering on obligations or rights envisaged under data protection legal regime.

International instruments

In 2007, the Heads of state and government within the ECOWAS adopted a Supplementary Act[18] to harmonize the existing regulatory framework and policies on information and communications technology (ICT) within the ECOWAS region and in recognition of the interdependence of ICT and data protection, the 2007 Act formed the basis for another *Supplementary Act on personal data protection*[19] (the Act) in Abuja on the 16th day of February, 2010 to regulate the 'collection, processing, transmission, storage and use of personal data' by public and private entities, etc. within the region. [20]

Prior to the adoption of the ECOWAS Act, four member states had enacted their respective national data protection laws without any influence from the ECOWAS region.[21] However, after the adoption, six other members have passed or issued data protection laws or regulations in fulfilment of their mandates under the ECOWAS Act to establish frameworks for data protection in their respective states[22] but this does not necessarily mean such laws were enacted in compliance with the dictates of the Act. For instance, the Act prescribes independence, immunity and oath of professional secrecy for members of data protection authorities (DPAs)[23] but under the Ghanaian Data Protection Act, for example, the DPA's members are solely appointed and sacked by the President of the country, they neither enjoy immunity nor subject to oath of secrecy.[24]

In Nigeria, although, the ECOWAS Act is sometimes considered as part of Nigeria's legal framework on data

15 Andrew U Iwobi, 'Stumbling Uncertainly into the Digital Age: Nigeria's Futile Attempts to Devise a Credible Data Protection Regime' (2016) 26(3) Transnational Law and Contemporary Problems 13.

16 Ife Ogunfuwa, 'Experts Call on Buhari to Assent Data Protection Bill' (2020) <https://punchng.com/experts-call-on-buhari-to-assent-data-protection-bill/> accessed 1 March 2021.

17 Uche Val Obi, 'An Extensive Article on Data Privacy and Data Protection Law in Nigeria' (2020) <https://eurocloud.org/news/article/an-extensive-article-on-data-privacy-and-data-protection-law-in-nigeria/> accessed 1 February 2021.

18 Supplementary Act A/SA.1/01/07 on the Harmonization of Policies and the Regulatory Framework for the ICT Sector.

19 Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, 2010 (ECOWAS Act).

20 See art 3(1), ECOWAS Act, 2010.

21 Cape Verde (2001; Burkina Faso (2004); Senegal (2008) and Benin (2009).

22 Ghana (2012); Cote d'Ivoire (2013); Mali (2013); Niger (2010); Togo (2019) and Nigeria (2019).

23 See arts 14–18, ECOWAS Act, 2010.

24 Ss 4(2) and 5(5), Data Protection Act, 2012.

protection, it has not been domesticated as of March 2021, hence not applicable in Nigeria by virtue of section 12 of the Nigerian Constitution, 1999 (as amended) which requires domestication of international treaties before they are enforceable in the country.[25]

The various legislative attempts by the Nigerian government at enacting a principal data protection Act have taken slight cognizance of the ECOWAS Act especially the draft Data Protection Bill 2020 which makes similar provisions on qualifications of a data protection commissioner as found in the ECOWAS Act.[26] Notwithstanding, its non-domestication, Nigeria is subject to the provisions of the Act before the regional courts which decisions play significant roles in policy making and implementation within the region.

African Union (AU) Convention on Cyber Security and Personal Data Protection (Malabo Convention). In its efforts to address Africa's need of a harmonized regulatory and legal framework for data protection, the African Union (AU), at its 23rd ordinary session in June 2014 adopted the Convention on Cyber Security and Personal Data Protection (Malabo Convention).[27]

Like Convention 108 in Europe,[28] the Malabo Convention represents Africa's international treaty regulating the processing of personal data by natural persons, states and local communities, public and private bodies identifying six identical principles with the eight in the GDPR. [29] The Malabo Convention mandates each African State to effectively set up legal frameworks strengthening fundamental rights, protection of physical data and privacy while simultaneously allowing a free flow of personal data on the continent.[30] However, the Malabo Convention is only comparable to Convention 108 in terms of their status as international treaties but it has not entered into force by virtue of its Article 36 which predicates enforcement on its ratification by fifteen member States but as of March 2021, only eight Member States had ratified, hence making the instrument yet unenforceable.[31]

Although Nigeria has neither signed nor ratified the Malabo Convention, its provisions colour Nigeria's data protection landscape either closely or remotely in terms of its harmonization of data protection framework in Africa. Without necessarily considering its enforceability with the Nigerian courts, the influence of Malabo Convention is impliedly acknowledged under the NDPR by its provision on development of 'international cooperation mechanism' and 'international mutual assistance'[32] and this provision is further strengthened by the NDPR Implementation Framework (Implementation Framework)[33] which prescribes resort to the Malabo Convention to cure any defect in the NDPR.[34]

General legislation

Although data protection in Nigeria is predominantly regulated by the Nigerian Constitution and the NDPR, some other statutes[35] and subsidiary legislation[36] are also relevant in this discourse.

25 See Uchenna Jerome Orji, 'Regionalizing Data Protection Law: A Discourse on the Status and Implementation of the ECOWAS Data Protection Act' (2017) 7(3) International Data Privacy Law179–89.

26 See art 15, ECOWAS Act, 2010.

27 African Union (AU) Convention on Cyber Security and Personal Data Protection was adopted in Malabo, Equatorial Guinea on the 27th day of June 2014 and signed by only 14 African member states (Benin, Chad, Comoros, Congo, Ghana, Guinea Bissau, Mozambique, Mauritania, Rwanda, Sierra Leone, Sao Tome and Principe, Togo, Tunisia and Zambia) as of March 2021. <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection> accessed 17 March 2021.

28 The Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108) was passed in 1980 by the Council of Europe. It is the first and only legally binding international instrument on data protection. See Colin J. Bennet, *The Council of Europe's Modernized Convention on Personal Data Protection: Why Canada Should Consider Accession* (Centre for International Governance and Innovation, 2020) 1.

29 Martha Kanene Onyeajuwa, 'Critical Assessment of Institutional and Regulatory Framework for Personal Data Protection in Digital Platform Ecosystem: A Study of Nigeria' (2018) 22nd Biennial Conference of the International Telecommunications Society (ITS): 'Beyond the Boundaries: Challenges for Business, Policy and Society', International Telecommunications Society (ITS), Calgary.

30 See art 8(1), AU Convention on Cyber Security and Personal Data Protection 2014.

31 Only Angola, Ghana, Guinea, Mozambique, Mauritius, Namibia, Rwandan, and Senegal have ratified. <https://au.int/sites/default/files/treaties/29560-slafrican_union_convention_ on_cyber_security_and_personal_data_protection.pdf> accessed 17 March 2021.

32 NDPR, reg 4.3(a) and (b).

33 This was issued as a guidance note by NITDA in November 2020 to give further clarity to the NDPR.

34 NDPR Implementation Framework, clause 16 recognises the persuasive effect of the Malabo Convention in Nigeria.

35 The Nigeria Police Act, 2020; the Federal Competition and Consumer Protection Act (FCCPA) 2019; the Companies and Allied Matters Act 2020; Child's Rights Act 2003; Labour Act LFN 1990; National Archives Act 1992; National Minimum Wage Act 2019; Employees Compensation Act 2010; Personal Income Tax (Amendment) Act 2011; Freedom of Information (FOI) Act 2011; National Identity Management Commission Act 2007; Trafficking of Persons (Prohibition) Enforcement and Administration Act 2015; Violence Against Persons Prohibition Act 2015; Administration of Criminal Justice Act 2015; HIV and AIDS Anti-Discrimination Act 2004; National Health Act 2004; Cybercrime (Prohibition, Prevention etc) Act 2015; Credit Reporting Act 2017; Official Secrets Act 1962; Money Laundering (Prohibition) Act 2003; Advance Fee Fraud and Other Fraud Related Offences Act 2006.

36 Apart from the principal legislation with data protection provisions, some regulators have also issued certain regulations or guidelines wholly or partly for the protection of personal data in their various sectors pursuant to the relevant enabling legislation. For lawyers and legal practice in Nigeria, the Rules of Professional Conduct for Legal Practitioners 2007 applies. In the banking sector, the Central Bank of Nigeria has invoked its regulatory powers under the Central Bank of Nigeria Act 2007 to issue a number of relevant guidelines for data protection to wit: Guidelines on Mobile Money Services 2015; Guidelines on Transaction Switching

From whatever prism data protection is viewed, its origin is traceable to information privacy guaranteed under the *Nigerian Constitution*.[37] Section 37 of same Constitution provides for privacy of citizens, homes, correspondence, etc and in 2014, the Court of Appeal in *Nwali v Ebonyi State Independent Electoral Commission (EBSIEC)*[38] expansively interpreted the provision to include all aspects of human life. Although the court did not particularly use the phrase 'data protection' in the judgment, academics and practitioners have on the other hand, argued that, the Nigerian Constitution is the foundation of all data protection provisions in Nigeria but this position is however suspect when it is considered that, while privacy under the Nigerian Constitution protects citizens, data protection on the other hand, universally, guarantees protection to residents. Conversely, since information privacy contemplates data protection, then section 37 of the Constitution continues to provide a source for data protection in Nigeria until a principal substantive legislative is enacted on the subject.

The Nigeria Data Protection Regulation 2019. In a historic move that set the tone for Nigeria's data protection landscape, NITDA—Nigeria's self-assigned national DPA, released the NDPR in 2019 to 'safeguard data privacy rights of natural persons, ensure a personal data during transaction are safely done, avert manipulation of personal data and ultimately ensure Nigeria business measure up to international data protection standards'.[39]

The NDPR in its extraterritorial scope, surprisingly applies to Nigerian citizens residing outside the country[40] even though enforcement of this audacious scope appears illusory, its propriety or otherwise is not the scope of this article. The regulation, reportedly draws its inspiration from the GDPR, however it stands out with its creation of enforcement agents in the mould of Data Protection Compliance Organizations (DPCOs) which are licensed by NITDA to co-ensure compliance with the NDPR.[41] The regulation however suffers from many problems in terms of: uncertainty surrounding NITDA's statutory powers to regulate data protection; the extraterritoriality of its scope without parameters for enforcement; conflation of American and European concepts of data privacy with data protection and personal data with personal identifiable data; omission of legitimate interest as one of the basis of lawful processing; confusion of data administrator with data processor; recognition of multiple data protection authorities and ultimately, the licensing regime of DPCOs instead of the preferred 'accreditation' which breeds less legitimacy problems.

Enforcement mechanism under the NDPR?

The GDPR's enforcement framework undoubtedly constitutes the highest standard of data protection system in today's world by placing a very high premium on compliance and enforcement.[42] Compliance with the provision of the GDPR is enforced at the national level by the respective Data Protection Authorities (DPAs) or Supervisory Authorities (SAs) which are accordingly advised by the European Data Protection Board subject to the European Commission's guidance.[43]

Prior to the issuance of NDPR, nothing worthy of note was recorded about institutional enforcement of data protection rights in Nigeria. There were neither general rules for administrative sanctions nor procedural guides for seeking redress in the court of law for data protection rights violation. This institutional deficiency was observed by World Bank thus:

> The benefits of digital platforms stem from their ability to virtually connect people and things, facilitating digital transactions/interactions, including the exchange of information, goods, and services. Despite some progress on the implementation of the goals of both the e-government Master Plan and ICT Road Map, much remains to be done in Nigeria, including institutional coordination, developing a Privacy and Data Protection Act, monitoring the quality of digital services, and fully embracing the Open Government Partnership.[44]

Services 2016; Regulatory Framework for Bank Verification Number Operations (BVN) Operations and Watchlist for the Nigerian Financial System 2017; Risk-Based Cybersecurity Framework 2018. For the telecommunications sector, Nigerian Communications Commission (NCC) also issued a number of regulations with data protection implications pursuant the enabling provision under the Nigerian Communications Act 2003 to wit: The Consumer Code of Practice Regulations 2007; Registration of Telephone Subscribers Regulations was issued in 2011; Internet Code of Practice was released in 2019. For the ICT sector, NITDA issued Guidelines for Nigerian Content Development in Information and Communication Technology (ICT).

37 The Constitution of the Federal Republic of Nigeria, 1999 (as amended) published in Gazette No. 27, Volume 83 of 5th day of May 1999.

38 (2014) LPELR - 23682 (CA).

39 NDPR, reg 1(1)(a)(d).

40 NDPR, reg. 1.2(b).

41 Diyoke Chika and Edeh Tochukwu, 'An Analysis of Data Protection and Compliance in Nigeria' (2020) 4(5) International Journal of Research and Innovation in Social Science 377.

42 Chris Jay Hoofnagle, Bart van der Sloot and Frederik Zuilderveen Borgesius, 'The European Union General Data Protection Regulation: What it is and What it Means'(2019) 28(1) ICTLJ 65; Abigayle Erickson, 'Comparative Analysis of the EU's GDPR and Brazil's LGPD: Enforcement Challenges With the LGPD' (2019) 44 Brook Journal of International Law 859.

43 GDPR, art 40, 50, 54–59, 61, 67, and 68.

44 World Bank Group, *N0igeria Digital Economy Diagnostic Report* (2019) <https://documents.worldbank.org/en/publication/documents-reports/

While appraising Nigeria's institutional framework for data protection, it is palpably evident that, Nigeria does not only need an effective data protection legislation but same must be complemented with a formidable system to run a seamless enforcement ecosystem for administrative sanctions and compensatory redress for victims.[45] However, the status quo appeared to have changed, albeit on paper, when the NDPR introduced a regulatory regime that requires filing of annual data protection compliance audit on behalf of data controllers by licensed DPCO, the creation of an Administrative Redress Panel (ARP) under the ultimate supervision of NITDA,[46] as well as the involvement of police and office of the Attorney General of the Federation in the enforcement cycle.

Data protection compliance audit

There is no gainsaying that the NDPR drew its inspiration from the GDPR where it picked data protection audit as a regulatory activity.[47] However, while under the European regulation, the supervisory authority only carries out an audit as part of investigatory activities on a need-basis, it is a mandatory annual exercise envisaged under the NDPR as a regulatory compliance indicator for data controllers.[48] Here, every data controller within a certain threshold of data processing activities is required to file an audit summary showing its data processing activities with a view to detecting existing gaps that would be plugged during a post-audit implementation exercise.[49]

The audit exercise is expected to be a thorough review and appraisal of the data controller's current data management standards after which an audit finding report ought to be filed with NITDA in March every year.[50] To demonstrate its baby steps in terms of regulatory compliance and enforcement, the NITDA reported that, 635 data controllers filed their annual audit between 2019 and 2020, however 17 out of the number were public bodies pointing to slow government participation in the process.[51] Empirical evidence is however lacking on how these annual audits have improved compliance with the provisions of the NDPR since the audit findings do not necessarily include remediation activation plans and especially since some categories of data controllers are exempted from filing such audits. A better approach to improve compliance, in addition to the audit requirement is, to register all data controllers in Nigeria and then ascertain their levels of compliance from their records kept with the supervisory authority as done in some jurisdictions.[52]

Data protection compliance organization

The NDPR defines a DPCO as 'any entity duly licensed by NITDA for the purpose of training, auditing, consulting and rendering services and products for the purpose of compliance with the NDPR or any foreign data protection law or regulation having effect in Nigeria'.[53] This provision superficially appears a novelty and pioneering one which introduced a new player into the institutional framework of data protection ecosystem. However, this assumption is not correct considering the provision of Article 41 of the GDPR which contemplates an accreditation system for competent bodies to perform some regulatory functions assigned to the supervisory authorities under European law.[54] While the word 'accredited' is used under the GDPR, NDPR provides for 'licence' enabling the DPCOs to, on behalf of NITDA, monitor, audit, train and consult for data controllers.[55] The NDPR's preference for licencing is problematic for its potential conflict with the provisions of the Legal Practitioners Act under which Nigerian

documentdetail/387871574812599817/nigeria-digital-economy-diagnostic-report> accessed 16 August 2021.

45 See Daniel U Unnam, 'Informational Privacy and Security Amid Growing Activities on Electronic Platforms in Nigeria: A Case for Data Protection Law' (2015) 6 Nnamdi Azikiwe University Journal of International Law and Jurisprudence 27; Bernard O Jemilohun, 'An Appraisal of Institutional Framework for Data Protection in the UK, USA, Canada and Nigeria' (2015) 1(1) Journal of Asian and African Social Science and Humanities 8–26.

46 Empirical research revealed that a higher percentage of Nigerian citizens could not trust the government with their privacy interests in the absence of a devoted legislation on privacy and data protection. See Tiwalade Adelola, Ray Dawson and Firat Batmaz, 'Nigerians' Perception of Personal Data Protection and Privacy' (SQM Conference 2015) <https://www.researchgate.net/publication/275968129_Nigerians'_Perceptions_of_Personal_Data_Protection_and_Privacy/citations> accessed 16 August 2021.

47 GDPR, art 58(1)(b).

48 NDPR, reg 4.1(7).

49 NDPR Implementation Framework 2020, clause 3.3.2. Data Controllers processing less than 2000 data subjects' personal data are exempted from filing annual audits. See reg 4.1(7) NDPR.

50 Although NITDA can also conduct scheduled audits, when necessary. See NDPR Implementation Framework, clause 6.1(a).

51 See NDPR Performance Report, 2019–2020.

52 For example, the English Information Commissioner (ICO) registers data controllers pursuant to the Data Protection (Charges and Information) Regulations 2018; s 27 of the Ghanaian Data Protection Act, 2012 provides for registration of data controllers and the Kenyan Data Protection Act 2019 also empowers the privacy commissioner to register data controllers and processors, see s 18.

53 NDPR, reg 1.3(xiii).

54 For the purpose of monitoring compliance with the GDPR, supervisory authorities in the EU are empowered to accredit competent bodies with demonstrable level of expertise in data protection, to carry out such functions as may be provided in a Code of Conduct. See Christopher Kuner and others, *The EU General Data Protection Regulation (GDPR). A Commentary* (OUP, Oxford, England, 2020) 725–31.

55 See NDPR, reg 4.1(4).

lawyers are licenced to provide legal services including the kind of advisory contemplated under the NDPR.

The population of data controllers and diversity of the Nigerian economy makes it almost impossible for NITDA to unilaterally monitor and ensure compliance with the NDPR, hence its designation of DPCOs to, during their audit exercises, evaluate the status of data controllers' compliance, appraise adequacy of protection offered to data subjects, identify current and potential non-compliance.[56] In reality, the DPCOs' duty of monitoring compliance is however tainted by the NDPR's provision that allows them to consult for data controllers in what appears to be a striking example of conflict of interest, where a compliance r organization plays the dual role of a prosecutor and counsel for an accused person and get paid in the process.

Administrative Redress Panel

Borrowing a leaf from rights of data subjects to lodge complaint with supervisory authorities as provided by Article 13(2)(d) GDPR, the NDPR mandates NITDA to set up an ARP to investigate allegations of data breaches and issue appropriate administrative orders.[57] Judging from its terms of reference, the Panel appears an investigative body empowered to issue orders and determine appropriate redress however, the NDPR is silent on whether the Panel can also issue fines.[58]

Although the NDPR creates the ARP without prejudice to data subjects' right to seek redress in court, the Federal High Court of Nigeria in the case of *Incorporated Trustees of Digital Rights Lawyers Initiative v Unity Bank Plc* has ruled that lodging a complaint at the ARP is a condition precedent which must be fulfilled before approaching the court.[59] This decision cannot however stand the test of appeal when the meaning of the phrase 'without prejudice' used in regulation 4.2(1) of the NDPR is considered since the appellate courts had in the past defined the phrase to mean 'without loss of any right'.[60] In resolving cases brought before the ARP, the applicable procedural rules are to be drawn by its panel of experts but as of May 2021, the ARP had not been set up by NITDA since it was neither referenced nor mentioned as part of the agency's achievements in the NDPR Performance Report published by NITDA in 2020.

National Information Technology Development Agency

Upon the approval of National Information Technology Policy (National IT Policy) in 2001, the NITDA was initially commissioned as an office with the main objective of provision of information communication technology tools to selected educational institutions in Nigeria.[61] It however became a statutory body upon the enactment of its enabling Act[62] in 2007 with express powers to, among other functions, coordinate and monitor information technology practices, develop guidelines for election governance (e-governance) and monitor use of electronic data interchange (EDI).[63]

In 2019, NITDA issued the NDPR which remains Nigeria's most comprehensive and wholly dedicated piece of legislation on data protection upon which the current legal framework is built. Unlike all other data protection laws which create their own supervisory authorities, NITDA as Nigeria's DPA, issued its own data protection subsidiary legislation and this explains the absence of clear provisions on the establishment, duties, obligations, independence, and modus operandi of the supervisory authority in the NDPR.[64]

In addition, under the NDPR, NITDA receives audit reports or conducts scheduled audits, issues licences to DPCOs, issues administrative fines, directs the ARP, makes adequacy decisions and may initiate criminal prosecution etc in the enforcement chain.[65] However, the NDPR Implementation Framework clearly refers to NITDA as the national data protection officer (DPO) and places it atop the enforcement chart without necessarily resolving the question on the identity of national DPA which is responsible for the enforcement of the NDPR.[66] This unsolved conundrum continues to cast aspersion on the NDPR, its legitimacy and enforcement mechanism.

These self-assigned functions of NITDA in relation to regulation of data protection do not however find support under section 6(a) and (c) of the NITDA Act which empower the agency to issue guidelines for e-governance and monitor EDI. E-governance is not data

56 NDPR, Implementation Framework, clause 6.5.

57 NDPR, reg 4.2(1).

58 All the provisions on issuance of fines in the NDPR and its Implementation Framework refer to NITDA.

59 (Unreported) Suit No FHC/AB/CS/85/2020 delivered by Ibrahim Watila, J. (of blessed memory) on 8 December 2020 in Abeokuta, Ogun State, Nigeria.

60 See the decision in *Federal Ministry of Health v The Trade Union Members of the Joint Health Sector Union* (2014) LPELR-23546 (CA).

61 Patience I Akpan-Obong, *Information and Communication Technologies in Nigeria; Prospects and Challenges for Development* (Peter Lang Publishing, Bern, Switzerland, 2009) 203; PC Obute, 'ICT Laws in Nigeria: Planning and Regulating a Societal Journey into the Future' (2014) 17 PELJ 1.

62 NITDA Act, 2007.

63 S 6 (a) and (c), NITDA Act 2007.

64 NITDA is simply referred to as 'The Agency'.

65 NDPR, reg 4.1.

66 Implementation Framework, clause 3.3.1.

protection and EDI is a merely device for exchange of business information, hence, power to issue guidelines on e-governance and monitor EDI ought not be confused with power to issue data protection regulation.

The Courts

Irrespective of the nature ascribed to data protection (whether fundamental right or tort) under the relevant laws, it is justiciable in the Nigerian courts.[67] Under the NDPR, victims of privacy rights violations can seek redress in court without prejudice to the proceedings of the ARP[68] and the Federal High Court of Nigeria ruled in *Incorporated Trustees of Laws and Rights Awareness Initiative v National Identity Management Commission (NIMC)*, that a data subject can legally sue for breach of his data under the NDPR.[69]

Although the NDPR does not specifically provide for any particular court with jurisdiction to enforce data protection rights, both the High Court of a State and the Federal High Court of Nigeria share concurrent jurisdiction. However, in two separate decisions delivered in 2020, the High Court of Ogun State erroneously declined jurisdiction over the NDPR in favour of the Federal High Court[70] but there exists no Court of Appeal decision on the status of the NDPR and the court with requisite jurisdiction to enforce data protection rights especially in the absence of a principal legislation on the subject.[71] Nigeria's case law on data protection is under-developed and the appellate courts are yet to take a definite position on the nature of data protection rights provided under the NDPR and this continues to hurt the growth of the concept in the country.[72]

The attorney general of the federation

One of the hallmarks of European data protection laws is the regulation of free flow of transfer of personal data between member countries based on agreed data protection principles.[73] Under the GDPR, personal data can be transferred to another country or international organizations where the European Commission has made an 'adequacy decision' on that country or organization except other safeguards exist.[74] Prior to the adoption of GDPR and after its commencement, the Commission had made decisions on some non-European Economic Area (EEA) countries with adequate data protection laws and drawn up a White list.[75]

In replicating this provision, NDPR requires the attorney general of the federation (AGF) to supervise transfer of personal data to 'foreign' countries and international organizations however NITDA or the AGF makes adequacy decisions on such foreign entities.[76] In his supervisory and enforcement role, the AGF may prohibit transfer of personal data to certain countries and grant fiat to NITDA to prosecute data breaches.[77] These provisions are however merely aesthetic and devoid of procedure for its activation. First, under the NDPR adequacy decisions are either made by NITDA or the AGF but the Implementation Framework subjects it to the directive of the latter. Second, unlike the GDPR that clearly sets out the conditions for adequacy decisions,[78] while the NDPR provides the consideration of legal system as the only condition, the Implementation Framework contemplates consideration of 'legal agreements' without providing clarity on its meaning. The most significant drawback of the provision is absence of guidelines on the application and decision process ie when is an application made?; who makes such application?; under what circumstance(s) is the application made?; how is the decision made?; what must the decision contain?; how is it communicated? etc.

67 See the decisions in *Nwali v Ebonyi State Independent Electoral Commission* (2014) LPELR 3682 (CA), *Habib Nigeria Bank Ltd v Fathudeen Koya* (1992) 7 NWLR (Pt 251) 43, *Emerging Market Telecommunication Service v Eneye* (2018) LPELR 46193(CA), *Godfrey Eneye v MTN Nigeria Communication* (Unreported) CA/L/136/2009, *Anene v Airtel Nig Ltd* (Unreported) FCT/HC/CV/545/2015 and *Joshua Agbi v MTN Nigeria* (Unreported) Suit No FHC/L/CS/1456/2018 where data protection in the technical sense was litigated under right to privacy.

68 NDPR, reg 4.2(1).

69 Per Watila, J (of blessed memory) in Suit No FHC/AB/CS/79/2020 at p 16.

70 See (Unreported) Suit No AB/83/2020 Digital Rights Lawyers Initiative (DRLI) v National Identity Management Commission (NIMC) and (Unreported) Suit No HCT/262/2020 and *Digital Rights Lawyers Initiative v LT Solutions Media Ltd*.

71 Suit No AB/83/2020, *DRLI v NIMC* has gone on appeal to the Ibadan division of the Court of Appeal in appeal number CA/IB/291/2020.

72 On the 28th day of January 2021, another judge refused to recognize data protection under right to privacy but rather held that a claim for the interpretation and construction of the provisions of the NDPR are not cognizable under fundamental rights. See (unreported) Suit No AB/207/2020, *DRLI v Rasaki, per Onafowokan, J.*

73 Eduardo Ustaran, *European Data Protection: Law and Practice* (IAPP, Portsmouth, New Hampshire, 2018) 436.

74 GDPR, art 45(2). See also Gregory Voss, 'Cross-Border Data Flows, the GDPR, and Data Governance' (2020) 29(3) Washington International Law Journal, 485.

75 Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay are all on the Whitelist.

76 NDPR, reg 2.11(a) and 2.12.

77 Implementation Framework, clauses 10.1.5, 14.1, 14.2.

78 Art 42(2) GDPR prescribes: rule of law and respect for human rights; existence and functioning of independent supervisory authority and international commitments.

Data protection officer

Just like its European counterpart, the NDPR envisages a layered approach to compliance and enforcement of data protection rights, hence its mandatory provision on designation of Data Protection Officers by data controllers.[79] However, the Implementation Framework untidily contradicts the NDPR on categories of data controllers that must appoint a DPO, meaning, not all controllers are duty bound to appoint one.[80] Although under the GDPR, a DPO is meant to be independent and report directly to highest management level in the company, he is not particularly accorded such latitude under the NDPR, but he is expected to ensure compliance with the regulation.[81]

The Implementation Framework requires every DPO to be knowledgeable in data protection, advise the controller on its obligations under the NDPR, monitor its compliance, liaise with the NITDA and DPCO on data protection issues.[82] With these tasks, the DPO occupies the lowest rung of the data protection enforcement system in Nigeria but the NDPR makes no provision on conflict of interest which makes a DPO susceptible to undue influence and directives from his appointors and thereby hindering his compliance duties.

Conclusion

This article has sketchily but amply beamed an academic spotlight on the legal and institutional landscape of data protection in Nigeria. In the process, I have concisely narrated the not-too-flowery background of data protection in Africa's largest economy by briefly identifying all the legislative attempts before the release of NDPR in 2019. I have also examined the major players in the enforcement mechanism, drawing similarities from Europe on form, rather than substance, especially since Nigeria has not recorded comparable success in terms of its enforcement drive. While Nigeria continues to wait for a principal legislation on data protection, it is hoped that the existing institutional framework will be optimally run by the respective players towards achieving the objectives of the NDPR until a principal law on data protection is enacted.

https://doi.org/10.1093/idpl/ipab023

79 European Data Protection Supervisor, *The Role of Data Protection Officers in Ensuring Effective Compliance with Regulation (EC) 45/2001* (Position Paper, 2005).

80 NDPR Implementation Framework, clause 3.4.1(a)–(d).

81 See GDPR, art 38(3) and NDPR, reg 4.1(2).

82 NDPR Implementation Framework, clause 3.7.