UNILAG LAW REVIEW

IN THE SHADOW OF THE GDPR: THE ROAD TOWARDS ADVANCING THE INFORMATION PRIVACY INTERESTS OF DATA SUBJECTS IN NIGERIA

Nancy Nkechinyere Stephen

Volume 5 No. 1 (2021)

IN THE SHADOW OF THE GDPR: THE ROAD TOWARDS ADVANCING THE INFORMATION PRIVACY INTERESTS OF DATA SUBJECTS IN NIGERIA

By Nancy Nkechinyere Stephen*

Following the enactment of the General Data Protection Regulation (GDPR) in 2016, the Nigerian government's Information Technology Development Agency (NITDA) released the Nigeria Data Protection Regulation (NDPR) in 2019 to address data privacy issues in the country. The NDPR, although possessing many similar compliance requirements to the GDPR, presents a framework for regulating data processing that is deficient in many ways when compared to the GDPR. A year after the NDPR was released, the Data Protection Bill (2020) was introduced into the Nigerian House of Representatives, which if passed, will close many of the gaps in the NDPR, while leaving some issues outstanding. Against this backdrop, in this paper, this writer assesses potential justifications for Nigeria's choice of a less stringent regulatory framework. These justifications include: the extraterritorial effect of the GDPR, the socio-economic climate in the country, and the role of the private sector in enhancing cybersecurity protection.

1.0. INTRODUCTION

Data protection is a topic of increasing interest in countries around the world. The rise in the processing of personal data for business purposes and governmental activities raises the question of to what extent these practices encroach on data subject privacy rights, even as the right to privacy is enshrined in the Constitution of most countries around the world. In accordance with the growing regulation of the data processing space, Nigeria issued the Nigeria Data Protection Regulation (NDPR) in 2019, which is the country's only comprehensive data protection regulation to date.[1] The

* Nancy Nkechinyere Stephen is a student at Columbia Law School (CLS), where she is a Richard Paul Richman Leadership Fellow. At CLS, she serves as a staff editor on the Columbia Journal of Transnational Law and is currently the President of the Law in Africa Students' Society. She is also a member of the Task Force for Diversity and Inclusion at the University and was recently named a Public Interest Honoree by the Law School for showing exceptional dedication to public service. After graduation, she will be working at WilmerHale, DC, United States as an associate lawyer. Email: nns2121@columbia.edu.

[1] DLA Piper, "Data Protection Laws of the World: Nigeria", available at https://www.dlapiperdataprotection.com/index.html?t=law&c=NG (accessed 3 February 2021).

Regulation, which was drafted with many similarities to the GDPR, has glaring substantial differences that may call into question its sufficiency. In response, commentators have rightly criticized the NDPR as providing inadequate protection for individual rights.[2] More recently, a Data Protection Bill was introduced to the House of Representatives to further tighten the data processing regulation standards and protect data subjects' rights in the country.[3] If passed, this Bill will close some of the gaps in the NDPR, but still leave some outstanding.

In Part I of this paper, this writer starts by discussing the urgency of the need for data protection in the world. Then, this writer proceeds to consider the GDPR as a cornerstone for other data protection laws in the world, including Nigeria's NDPR, and ends by focusing on the legal framework for data protection in Nigeria, which is primarily the NDPR. This writer also introduces a discussion of the Data Protection Bill, which will likely supplement the NDPR.

In Part II, this writer compares and contrasts the NDPR to the GDPR, focusing on provisions of the NDPR that substantially deviate from the GDPR. At the same time, this writer provides commentators' critiques of some of the NDPR's deviations. Next, this writer discusses the ways the Data Protection Bill closes some of the identified gaps in the NDPR through a comparison of the Bill to the Regulation.

Having determined that majority of the gaps in the NDPR will likely be closed by the Data Protection Bill (2020), in Part III this writer discusses potential justifications for the nature of Nigeria's data protection regime. To do this, this writer discusses the ways in which the GDPR's extra-territorial effect bridges some outstanding gaps in the Data Protection Bill as it relates to foreign and multinational Nigerian businesses. Next, with respect to local/territorial businesses and the Nigerian government – both of which are uncovered by the GDPR – this writer explains reasons why Nigeria may has chosen a

[2] *See* Part II of this Paper.

[3] OneTrust DataGuidance, "Nigeria: NITDA Publishes Draft Data Protection Bill 2020 for Public Comments", available at https://www.dataguidance.com/news/nigeria-nitda-publishes-draft-data-protection-bill-2020-public-comments (accessed 3 February 2021).

looser framework to regulate their data processing activities. This includes a discussion of Nigeria's socio-economic status and ways in which the private sector has been effective in closing gaps in the NDPR that are also present in the Data Protection Bill. At each stage of the Part III discussion, this writer highlights issues with Nigeria's data protection regime that persists, despite the potential justifications for the looser framework and propose several amendments to address these lapses.

This paper brings to light important considerations for the strengthening of the Nigerian legal framework for data protection. The Data Protection Bill is currently being considered by the House of Representatives and takeaways from this discussion can be used to further equip legislative advocates with the information they need in recommending any changes to the Bill.

2.0. THE URGENCY OF DATA PROTECTION

Data is the oil of the digital era.[4] The generally accepted view is that "data is the key to unlocking customer value."[5] Data from 2019 shows the high popularity amongst businesses of use of customer data to predict trends in retail.[6] Also, PricewaterhouseCoopers'(PWC) 22nd Annual Global CEO survey shows that an overwhelming amount of CEOs consider data on customer and client preferences as critical or important.[7] There has also been a recent increase worldwide in government demands for data held by the private sector, including an expansion in government requests for direct access by the government to private-sector databases or networks; or government access to large volumes of data.[8] With the rising use of data for

[4] The Economist, "The World's Most Valuable Resource is no Longer Oil, but Data", available at https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (accessed 3 February 2021).
[5] F. Ololuo, "Data Privacy and Protection under the Nigerian Law", available at http://www.spaajibade.com/resources/data-privacy-and-protection-under-the-nigerian-law-francis-ololuo/ (accessed 3 February 2021).
[6] *Ibid.*
[7] PwC, "23rd Annual Global CEO Survey", available at https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2019/gx.html (accessed 3 February 2021).
[8] I.S. Rubinstein, G.T. Nojeim, R.D. Lee, "Systematic Government Access to Personal Data: A Comparative Analysis" (2014) 4(2) *International Data Privacy Law*, p. 96.

business strategy analytics and governmental functions, there is a growing global concern about the potential for company and government misuse or abuse of individuals' personal information, including sensitive personal data like criminal conviction records.[9] There is also concern about the potential for anonymous individuals to hack into company databases and steal sensitive information and harm consumers, i.e. through fraud and identity theft.[10] Led by the EU, governments have begun responding to these concerns with increased regulation of data collection and processing activities and data security procedures.[11]

2.1. The Role of the GDPR as a Cornerstone to Other Countries' Data Privacy Regulations

As early as the 1990s, the EU passed a Data Protection Directive (Directive 95/46/EC) to protect its citizens against possible abuses of their personal data.[12] Years later, advancements in technology changed the way data was handled and a review of the existing rules became necessary.[13] In response, the EU enacted the General Data Protection Regulation (GDPR) in 2016 and it came into effect in 2018.[14] The GDPR "regulates the processing by an individual, a company or an

[9] C.D. Raab, "The Governance Of Global Issues: Protecting Privacy in Personal Information", in *New Modes of Governance in Global System*, p. 125, available at https://link.springer.com/chapter/10.1057/9780230372887_6 (accessed 11 May 2022); *see also* R. Kirpatrick, "Unpacking the Issue of Missed Use and Misuse of Data", available at https://www.unglobalpulse.org/2019/03/unpacking-the-issue-of-missed-use-and-misuse-of-data/ (accessed 3 February 2021).

[10] R. Sobers, "134 Cybersecurity Statistics and Trends for 2021", available at https://www.varonis.com/blog/cybersecurity-statistics/ (accessed 3 February 2021).

[11] Kirpatick, *supra* n 9.

[12] *See* Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046 (accessed 3 February 2021).

[13] Privacy Europe, "European Privacy Framework", available at https://www.privacy-europe.com/european-privacy-framework.html#:~:text=History,gathering%20data%20about%20their%20customers (accessed 3 February 2021).

[14] GDPR.EU, "What is GDPR, the EU's New Data Protection Law?", available at https://gdpr.eu/what-is-gdpr/ (accessed 3 February 2021).

organisation of personal data relating to individuals in the EU."[15] It provides data subjects with several privacy rights and requires entities processing data to abide by seven data protection and accountability principles.[16] These include: accountability; lawfulness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability.[17]

The GDPR became a cornerstone for several national laws outside of the EU, with each country enacting a modified version of the GDPR based on its attitude towards privacy. Countries with laws like the GDPR include Chile, Japan, Brazil, South Korea, India, New Zealand, Thailand, the US (particularly, California), Australia, China, Kenya, and most importantly, Nigeria.[18]

2.2. The Legal Framework of Data Privacy and Protection Laws in Nigeria

Following the enactment of the GDPR and in line with growing global concerns about data privacy, the National Information Technology Development Agency (NITDA) promulgated the Nigeria Data Protection Regulation (NDPR).[19] Like many other countries, privacy in Nigeria is a Constitutional right and there are existing statutes that contain age/industry specific privacy protections.[20] These Nigerian statutes include: The Child Rights Act 2003; The NCC Consumer Code of Practice Regulation 2007; The National Identity Management Commission (NIMC) Act 2007; The NCC Registration of Telephone Subscribers Regulation 2011; The Freedom of Information Act 2011; The National Health Act (NHA) 2014; The Cybercrimes (Prohibition,

[15] European Commission, "What Does the General Data Protection Regulation (GDPR) Govern?", available at https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_en (accessed 3 February 2021).
[16] *Supra* n 14.
[17] *Ibid.*
[18] D. Simmons, "12 Countries with GDPR-like Data Privacy Laws", available at https://insights.comforte.com/12-countries-with-gdpr-like-data-privacy-laws (accessed 3 February 2021). *See* Part II of this Paper for a discussion of Nigeria's data privacy laws.
[19] Nigeria Data Protection Regulation (2019).
[20] F. Ololuo, "Nigeria: Data Privacy and Protection under the Nigerian Law", available at https://www.mondaq.com/nigeria/privacy-protection/895320/data-privacy-and-protection-under-the-nigerian-law (accessed 3 February 2021).

Prevention, etc.) Act 2015; The Consumer Protection Framework 2016; and The Federal Competition and Consumer Protection Act 2019.[21] To date, the only law comprehensively regulating data privacy in Nigeria is the NDPR, which was passed in 2019. However, the Data Protection Bill (newly introduced into the House of Representatives), if passed, will augment the existing framework for data protection in Nigeria.

2.3. Understanding the NDPR

2.3.1. NITDA's Authority to Enforce

The NITDA promulgated the NDPR using power from its statutory mandate under the National Information Technology Development Agency Act (2007), which states in relevant part that NITDA shall:

> Create a framework for the…regulation of Information Technology practices, activities and systems in Nigeria and all matters related thereto and for that purpose[22]…Develop guidelines for electronic governance and monitor the use of electronic data interchange and other forms of electronic communication transactions[23]…and introduce appropriate regulatory policies and incentives to encourage private sector investment in the information technology industry.[24]

2.3.2. The Objectives of the NDPR

The objectives of the NDPR are as follows:

a. to safeguard the rights of natural persons to data privacy;
b. foster safe conduct for transactions involving the exchange of Personal Data;
c. to prevent manipulation of Personal Data; and

[21] *Ibid.*
[22] National Information Technology Development Agency Act (2007), Part II, section 6(a).
[23] *Ibid*, at section 6(c).
[24] *Ibid*, at section 6(i).

d. to ensure that Nigerian businesses remain competitive in international trade through the safeguards afforded by a just and equitable legal regulatory framework on data protection and which is in tune with best practice."[25]

In accordance with its objectives, the NDPR consists of elements that give some level of data protection to the data subjects and provides data management compliance requirements for businesses, in ways like the GDPR. Key highlights of the NDPR are as follows: (i) The Regulation requires covered entities to provide data subjects with their privacy policy and requires that the policy contain certain provisions;[26] (ii) Covered entities are required to develop security measures to protect individuals' data;[27] (iii) Data controllers are required to communicate information related to data processing to data subjects in a clear manner;[28] (iv) Data processing by a third party is to be governed by a written contract;[29] (v) Transfer of Personal Data to a foreign country may be allowed where NITDA has decided that the affected country ensures adequate data protection;[30] (vi) Processing of data is lawful in certain specified circumstances;[31] (vii) Consent is one of the lawful basis for obtaining and processing personal data and must be informed, freely given, and unambiguous;[32] (viii) No consent shall be sought, given or accepted in any circumstance that may engender propagation of atrocities, hate, child rights violation, criminal and antisocial acts;[33] (ix) Personal data should be adequate, accurate and without prejudice to the dignity of human person.[34] It should also be stored only for the period within which it is reasonably needed;[35] (x) Maximum penalty for breaches of data

[25] *Ibid*, at Part I, section 1.
[26] KPMG, "The Nigeria Data Protection Regulation: Journey to Compliance", available at https://assets.kpmg/content/dam/kpmg/ng/pdf/advisory/NDPR-journey-to-compliance.pdf (accessed 3 February 2021).
[27] *Ibid.*
[28] *Ibid.*
[29] *Ibid.*
[30] *Ibid.*
[31] *Ibid.*
[32] *Ibid.*
[33] *Ibid.*
[34] *Ibid.*
[35] *Ibid.*

privacy rights on international transfers can be up to 10 million naira or 2% of annual gross revenue of the preceding year, whichever is higher and based on the number of Data Subjects dealt with.[36]

Despite these attributes of the NDPR, the Regulation is amiss in certain respects especially when compared to the GDPR.[37]

2.4. The Data Protection Bill (2020)

Currently, there is a draft Data Protection Bill (DPB) before the National Assembly, proposed by the NITDA.[38] If passed, it would close some of the gaps in the NDPR. The DPB was drafted in furtherance of Nigeria's Digital Identification for Development (ID4D) Project.[39] The project's goal is to establish a central digital identification system, enrolling residents and Nigerians abroad.[40] As one of the requirements for the execution of this project, Nigeria is to strengthen the legal institutional framework governing data protection.[41] The World Bank imposed this requirement on Nigeria in recognition that a central identification system can be "detrimental to data privacy and protection."[42] In light of this, the DPB's objectives slightly differ from that of the NDPR and its content is more similar to the GDPR.[43]

---

[36] *Ibid.*
[37] For a discussion, see Part II of this Paper.
[38] J. Daniel, "Nigeria Data Protection Bill Aims to Reinforce Information Security Rules", available at https://www.cio.com/article/3586844/what-you-need-to-know-about-nigerias-new-data-protection-bill.html (accessed 3 February 2021).
[39] World Bank Group, "Nigeria Digital Identification for Development (ID4D): Project Sheet", available at https://financeincommon.org/sites/default/files/2020-11/ID4D.pdf (accessed 3 February 2021).
[40] *Ibid.*
[41] The World Bank, "Nigeria Digital Identification for Development", available at https://projects.worldbank.org/en/projects-operations/project-detail/P167183 (accessed 15 February 2021).
[42] World Bank, "International Development Association Project Appraisal Document on a Proposed Credit in the Amount of SDR 84.4 Million to the Federal Republic of Nigeria for the Digital Identification for Development Project", available at http://documents1.worldbank.org/curated/en/250181582340455479/text/Nigeria-Digital-Identification-for-Development-Project.txt (accessed 3 February 2021).
[43] For a discussion, see Part II of this Paper.

Notably, the DPB removes the objective that Nigerian businesses remain competitive in international trade;[44] this aim was a key consideration in drafting the NDPR.[45] The DPB still serves to promote a code of practice that ensures personal data privacy without unduly undermining the legitimate interests of commercial organizations and government security agencies.[46]

3.0. A COMPARISON OF THE EU (GDPR) AND NIGERIAN DATA PROTECTION REGIMES (NDPR & DPB): ANALYSIS AND CRITIQUES

The GDPR is an effective point of comparison for Nigeria's data privacy regulations due to the *Brussels Effect*.[47] The *Brussels Effect* is a term coined by Anu Bradford in one of her written works.[48] It refers to Europe's unilateral power to regulate global markets,[49] setting the global rules across a range of areas including *the protection of privacy*.[50] In her book, Bradford explains that the EU wields this unilateral influence for various reasons. The first reason is its market power; the EU has a large consumer population, with 500 million consumers.[51] The second is due to Europe's regulatory capacity to translate its market power into tangible regulatory influence.[52] The third reason for the EU's unilateral influence is because of its preference for strict

---

[44] *See* Nigeria Data Protection Bill 2020, section 1.1.

[45] P. Ifeoma, "Issues Arising from the Nigerian Data Protection Regulation 2019 (Part 2) – Femi Daniel", available at https://dnllegalandstyle.com/2019/issues-arising-from-the-nigerian-data-protection-regulation-2019-part-2-femi-daniel/ (accessed 3 February 2021).

[46] *See* Nigeria Data Protection Bill 2020, section 1.1(a).

[47] A. Bradford, "The Brussels Effect – How the European Union Rules the World", available at https://oxford.universitypressscholarship.com/view/10.1093/oso/9780190088583.001.0001/oso-9780190088583 (accessed 11 May 2022).

[48] A. Bradford is a Professor of Law at Columbia University.

[49] *Supra* n 47, at p. 26.

[50] *Ibid*. at p. 34.

[51] *Ibid*, at pp. 26 and 34. Note that the assertion that the EU has 500 million consumers is from a 2012 data. Currently, the EU has 446 million inhabitants, which is still very large. *See* European Union, "Living in the EU", available at https://europa.eu/european-union/about-eu/figures/living_en#:~:text=The%20EU%20covers%20over%204,population%20after%20China%20and%20India (accessed 3 February 2021).

[52] *Supra* n 47, at p. 30.

rules;[53] the EU has more stringent privacy regulations.[54] The fourth is that the EU's regulations cannot be circumvented by moving the regulatory targets to another jurisdiction;[55] the EU's privacy standards already affect the business practices of many non-EU companies, including some operating in Nigeria.[56] The fifth reason is the focus of its regulations on inelastic markets like data privacy.[57] For example, the GDPR applies to all companies processing personal data of data subjects residing in the EU, regardless of where the data processing takes place or where the company processing the data is located.[58] The final reason, which Bradford discusses, is legal or technical non-divisibility.[59] In the case of data protection regulations, technical non-divisibility applies because of the difficulty of separating a company's data services across multiple markets for technological reasons.[60]

In view of the *Brussels* Effect, in this section, to shed light on some issues with Nigeria's data protection framework, this writer will be comparing the country's data protection regime – the NDPR, and the soon to be enacted DPB – to the EU's data protection regime, encapsulated in the GDPR.

4.0. Differences between the GDPR and the NDPR[61]

While the NDPR and the GDPR harbour many similarities, there are some substantial differences, some of which have been criticized by Nigerian scholars. They are discussed below.

---

[53] *Ibid*, at p. 37.
[54] M. Nadeau, "General Data Protection Regulation (GDPR): What you Need to Know to Stay Compliant", available at https://www.csoonline.com/article/3202771/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html (accessed 3 February 2021).
[55] *Supra* n 47, at p. 16.
[56] *Ibid*. at p. 23.
[57] *Ibid*, at p. 48.
[58] *Ibid*, at p. 49
[59] *Ibid.* at p. 53.
[60] *Ibid.* at p. 57.
[61] For an overview of the differences and similarities between the GDPR and NDPR, see generally OneTrust Data Guidance, "Comparing Privacy Laws: GDPR v. Nigerian Data Protection Regulation", available at https://www.dataguidance.com/resource/comparing-privacy-laws-gdpr-v-nigerian-data-protection-regulation (accessed 3 February 2021).

4.1. NDPR material scope

4.1.1. Scope of Data Protection

The GDPR applies to the processing of personal data by automated means or non-automated means if the data is part of a filing system.[62] Article 2 of the GDPR stipulates that the Regulation applies to "the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system."[63]

However, the NDPR only applies to the processing of personal data by automated means.[64] Section 1.3(iv) of the NDPR defines "data" as "characters, symbols, or binary on which operations are performed on a computer."[65] The NDPR's chosen definition limits the scope of its protection to personal data stored electronically. Critiques of the NDPR's approach rightfully highlight that the computer-centric nature of the definition of "data" defeats the Regulation's objective to safeguard Nigerians' privacy rights. Bisola Scott and Sandra Eke assert that it is necessary to amend the provisions of the NDPR to expressly regulate the processing of non-electronic or paper-based data.[66] They base their argument on the fact that "in Nigeria the paper shredding culture is poor and on a daily basis volumes of personal and sensitive paper documents are utilized without adequate security defences."[67] Olumide Babalola, a Technology attorney and outspoken critique of the NDPR, also argues that not only is the definition of data "narrowly

---

[62] *Ibid*, at p. 9.
[63] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) Article 2(1).
[64] *Supra* n 3.
[65] Nigeria Data Protection Regulation 2019, section 1.3(iv).
[66] B. Scott and S. Eke, "Nigeria: NITDA's Power to Regulate Non-Electronic Data", available at http://www.spaajibade.com/resources/nitdas-power-to-regulate-non-electronic-data-bisola-scott-and-sandra-eke/ (accessed 3 February 2021). Scott and Eke importantly note that while the narrow definition of "data" is not ideal, NITDA, the drafters of the NDPR, do not have the power to regulate non-electronic data.
[67] *Ibid*.

technical," it is also "not comprehensive enough in light of the Regulation's expectations [to protect a wide range of personal data]."[68] He further notes that the narrow definition of "data" in the NDPR can come in handy for "mischievous data controllers" seeking to misuse customer data.[69]

4.1.2. Special requirements for the processing of sensitive data

The GDPR provides special protection for the processing of sensitive personal data, including criminal records, while the NDPR does not offer similar protections. In the GDPR, articles 9 and 10 discuss "sensitive data." Article 9 allows for the processing of sensitive data only in certain specified circumstances.[70] It describes sensitive data as information revealing:

> Racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning sex life or sexual orientation.[71]

Article 10 further provides special protections for personal data pertaining to criminal convictions or offences;[72] this provision is most likely in recognition that criminal records checks can be "significantly intrusive, excessive and disproportionate to the (public interest) needs."[73] The EU Regulation specifically requires that the processing of personal data relating to criminal convictions and offences shall only be carried out under the control of "official authority" or where such

---

[68] U. Chioma, "My Thoughts on The Nigeria Data Protection Regulation (NDPR) 2019 By Olumide Babalola", available at https://thenigerialawyer.com/my-thoughts-on-the-nigeria-data-protection-regulation-ndpr-2019-by-olumide-babalola/ (accessed 3 February 2021).

[69] *Ibid*.

[70] *See* Regulation (EU) 2016/679, *supra* n 63, at Article 9.

[71] *Ibid*, at Article 9(1).

[72] *Ibid*, at Article 10.

[73] R. Finn, "Criminal Records Checks in Employment Contexts: Old and New Obligations under Data Protection Law", available at https://www.trilateralresearch.com/criminal-records-checks-in-employment-contexts-old-and-new-obligations-under-data-protection-law/ (accessed 3 February 2021).

processing has been "authorized by European law or that of any EU Member State *providing for appropriate safeguards for the rights and freedoms of data subjects*."[74] Additionally, the Regulation requires that "any comprehensive register of criminal convictions is to be kept only under the control of *official authority*."[75]

On the other hand, while the NDPR provides for a definition of sensitive data like that in the GDPR,[76] it does not provide special protections for sensitive personal data. Criminal conviction records are also not covered under the NDPR.

4.2. International Data Transfers (NDPR)

The GDPR contains more stringent requirements for personal data protection than the NDPR in cases of international transfers. Under the GDPR, if there is no decision on the adequate level of protection for personal data from the EU Commission, an international transfer is permitted when the data controller or data processor provides appropriate safeguards and on the condition that effective legal remedies that ensure data subjects' rights are obtainable.[77] Appropriate safeguards include: binding corporate rules (BCRs)[78] with specific requirements; standard contractual clauses adopted by the EU Commission[79] or by a supervisory authority; an approved code of conduct; or an approved certification mechanism.[80]

---

[74] Regulation (EU) 2016/679, *supra* n 63, at Article 10.
[75] *Ibid*.
[76] *See* Nigeria Data Protection Regulation 2019, section 1.3(xxv).
[77] *See* Regulation (EU) 2016/679, *supra* n 63, at Article 46.
[78] According to the GDPR, BCRs are "personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity." *See* Regulation (EU) 2016/679, *supra* n 63, at Article 4.
[79] The EU has issued three sets of standard contractual clauses. Two for transfers from EU controllers to non-EU controllers and 1 for transfers from EU controller to non-EU processors. See generally EU Commission, "Standard Contractual Clauses for Data Transfers between EU and non-EU Countries", available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en (accessed 3 February 2021).
[80] *See* Regulation (EU) 2016/679, *supra* n 63, at Article 46(2).

In contrast, where there is no approval on the adequate level of protection for personal data transfer by the NITDA or other regulatory bodies, the NDPR takes a less protective approach in specifying the "necessary" circumstances in which transfers would still be permissible.[81] Particularly, the Regulation permits transfers, in relevant part, "for the establishment, exercise or defence of legal claims", and "in order to protect the vital interests of the data subject *or of other persons* [for cases where a data subject is legally or physically incapable of giving consent]."[82] Without clarity on whose legal claims are to be considered for international transfers and which "other persons" interests are to be considered, the NDPR's approach in this respect is less protective of data subjects' rights.

4.3. Data Processing Records (NDPR)

The GDPR requires data controllers and data processors to maintain a record of processing activities under their responsibility and provides exceptions for small organizations.[83] It also prescribes a list of information that data controllers must record for international transfers of personal data.[84] Whereas, the NDPR does not impose any obligation to maintain a record of processing activities on data processors and controllers. The absence of such a requirement in the NDPR could make it more difficult for the NITDA to keep track of covered entities' compliance with their processing obligations. This in turn significantly diminishes the agency's ability to collect hard evidence when investigating companies for violations of the Regulation.

4.4. Data Security and Breaches (NDPR)

The GDPR requires data controllers to notify the supervisory authority of a high-risk personal data breach, where feasible, no later than 72 hours after having become aware of the breach.[85] The Regulation also requires data controllers to notify data subjects of the

[81] *See* Nigeria Data Protection Regulation 2019, section 2.12.
[82] *Ibid*, at section 2.12 (d)-(f).
[83] *See* Regulation (EU) 2016/679, *supra* n 63, at Article 30.
[84] *Ibid.*
[85] *See* Regulation (EU) 2016/679; *supra* n 63, at Article 33.

breach without undue delay.[86] However, the NDPR does not provide any reporting requirements. Commentators have critiqued the absence of reporting requirements in the NDPR. Diyoke Michael Chika and Edeh Stanley Tochukwu, Sociology and Computer Science Professors at Nigerian universities, argue that the NDPR's failure to require data controllers to notify data subjects of breaches inhibit data subjects' ability to take necessary actions to protect themselves from possible misuse and abuse of their personal data.[87] Additionally, Oruaro Ogbo, a writer for Stears Business,[88] further argues that without reports from businesses on substantial data breaches, the NITDA would be unable to analyze trends in breaches, discover themes, and share its findings.[89] This also prevents opportunities for Nigerian companies to learn from the mistakes of their peers and fortify their data protection measures appropriately.[90]

4.5. Accountability (NDPR)

4.5.1. Approach to Ensuring Accountability of Data Processors and Controllers

Both the GDPR[91] and the NDPR[92] recognize accountability as a core principle, but the NDPR adopts a more relaxed language in imposing the obligation of accountability on data processors and controllers.

The GDPR requires DPIAs (Data Protection Impact Assessments) to be conducted for envisaged high risk processing operations that use new technologies.[93] DPIAs are processes that help businesses identify

[86] *Ibid*, at Article 34.
[87] D.M. Chika and E.S. Tochukwu, "An Analysis of Data Protection and Compliance in Nigeria", (2020) 5(4) *International Journal of Research and Innovation in Social Science*, pp. 377 and 380.
[88] O. Ogbo, "Nigeria's Cybersecurity Problem", available at https://www.stearsng.com/article/nigerias-cybersecurity-problem#:~:text=It%20turns%20out%20that%20Nigeria,about%20%24270%20million%20on%20cybersecurity (accessed 3 February 2021).
[89] *Ibid*.
[90] *ibid*.
[91] See Regulation (EU) 2016/679, *supra* n 63, at Article 5.
[92] Nigeria Data Protection Regulation 2019, section 2.1(3).
[93] See Regulation (EU) 2016/679, *supra* n 63, at Article 35.

and minimize the data protection risks of a project.[94] The GDPR particularly requires these assessments when handling sensitive data and in some other cases of systematic monitoring or evaluation of data.[95] The GDPR also stipulates baseline requirements for DPIAs – they are to include intended measures to address the risks identified and mechanisms to ensure compliance with the GDPR and ensure the protection of personal data.[96] Furthermore, the GDPR stipulates several requirements with respect to the content of processor contracts.[97]

The NDPR, on the other hand, applies a loose approach to ensuring accountability when processing high risk data with new technologies. The text of the Regulation simply states that businesses are to conduct an audit covering the "impact of technology on privacy and security policies,"[98] without imposing baseline requirements or giving any guidance to businesses on what is to be included in audits covering privacy impacts. It also does not expressly require that audits contain information on risks to consumer data protection. Additionally, as opposed to expressly laying out requirements for the content of processing contracts, the NDPR simply imposes the obligation of a party to any processing contract, apart from the data subject, to take measures to ensure that the other party has not violated the data subjects' rights.[99]

4.5.2. Obligation for Data Controllers to Provide Representative in Country

For accountability purposes, the GDPR requires data controllers and processors to have their designated representative within the EU,

---

[94] Information Commissioner's Office (ICO) "Guide to the General Data Protection Regulation (GDPR): Data Protection Impact Assessments, ICO (UK)", available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/#:~:text=A%20Data%20Protection%20Impact%20Assessment,some%20specified%20types%20of%20processing (accessed 3 February 2021).
[95] *See* Regulation (EU) 2016/679, *supra* n 63, at Article 35(3).
[96] *Ibid*, at Article 35(7).
[97] *Ibid*, at Article 28(3).
[98] Nigeria Data Protection Regulation 2019, section 4.1(5)(j).
[99] *Ibid*, at section 2.4(b).

except where processing is occasional; does not largely include processing of sensitive data; or is low-risk to data subjects.[100] The representative is to be addressed to supervisory authorities and data subjects on all issues related to processing, for the purposes of ensuring compliance with the GDPR.[101] However, under the NDPR there is no obligation for covered entities to designate a representative within Nigeria. The combined absence of reporting and local-representative requirements will make it more difficult for the NITDA officials to closely monitor the processing activities of international data processors and controllers.

4.5.3. Independence of Supervisory Authority

The GDPR requires that supervisory authorities in EU member states act with "complete independence" in performing their tasks and powers in accordance with the Regulation.[102] This entails that members of each supervisory authority are to refrain from any action or occupation incompatible with their duties.[103] The word "incompatible" could be read to mean occupations that result in a conflict of interest, such as simultaneously working for the government, which handles citizens' data through its agencies and cabinets, and for private institutions that engage in data processing activities. On the other hand, the NDPR does not provide for an independent supervisory authority. Rather, the NITDA, an agency of the Federal Government, oversees compliance with the Regulation.[104] The NITDA's non-independence raises questions about its ability to objectively monitor and review the government's processing of personal data.

[100] *See* Regulation (EU) 2016/679, *supra* n 63, at Article 27(2).
[101] *Ibid,* at Article 27(4).
[102] *Ibid*, at Article 52.
[103] *Ibid*, at Article 52(4).
[104] National Information Technology Development Agency Act 2007, Part II, section 2.

4.6. Children's Data (NDPR)

While both the NDPR[105] and GDPR[106] require that data controllers provide information addressed to children in "clear and plain language," the GDPR imposes additional requirements to ensure the security of children's data.

Recital 75 of the GDPR emphasizes that children are "vulnerable natural persons."[107] Recital 38 of the GDPR further states that children require specific protection with regard to their personal data.[108] In line with these assertions, the GDPR requires data controllers to receive the consent of a parent or guardian for the processing of data for children under the age of 16.[109] The controllers are also required to make "reasonable efforts" to verify that the consent was indeed given by the children's parent or guardian.[110]

The NDPR does not impose additional protections for the processing of children's data and in response, commentators have criticized the Regulation.[111] This is because of the problems surrounding children's data privacy in Nigeria. In 2014, a study conducted by Consumers International found that one of the primary concerns of data collection in Nigeria is that children are exposed to privacy risks online and may unknowingly disclose personal information to online platforms due to the appealing nature of their visual content.[112]

[105] Nigeria Data Protection Regulation 2019, section 3.1(1).
[106] *See* Regulation (EU) 2016/679, *supra* n 63, at Article 12(1).
[107] *Ibid*, at recital 75.
[108] *Ibid*, at recital 38.
[109] *Ibid*, at Article 8.
[110] *Ibid.*
[111] A. Adeyoju, "A Quick Guide on the Data Protection Regime in Nigeria", available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3522188 (accessed 3 February 2021).
[112] D. Igbebulem, "The Protection of Consumers' Personal Data in the Era of E-commerce in Nigeria", available at https://www.researchgate.net/publication/334837471_The_Protection_of_Consumers'_Personal_Data_in_the_Era_of_E-commerce_in_Nigeria (accessed 3 February 2021).

4.7. Remedies (NDPR)

Compared to the GDPR, the NDPR offers more limited rights to data subjects attempting to access remedies for violations of their stipulated rights in three ways:

First, while both the GDPR and NDPR give data subjects the right to lodge a complaint with the supervisory authority for violations of their rights, the GDPR allows data subjects to better track the status of their complaints. Under Article 77.2 of the GDPR, the supervisory authority is required to inform the complainant, i.e. data subject, about the progress and outcome of their complaint including the possibility of a judicial remedy.[113] The NDPR, on the other hand, does not expressly provide data subjects with the right to receive information on the progress of their complaints.

Second, the GDPR provides individuals with a cause of action for violations of their rights under the Regulation. It also provides data subjects with the right to effective judicial remedy.[114] Also, in Article 82, the GDPR gives data subjects the right to receive compensation from the controller or processor for damages suffered.[115] By contrast, the NDPR only gives data subjects the right to lodge a complaint with the NITDA for any alleged violations of their rights.[116]

Third, unlike the NDPR, article 80 of the GDPR gives data subjects the right to representation by a not-for-profit organisation that advocates for the protection of data subject rights with regards to their personal data.[117] The organisations can lodge a complaint on the data subject's behalf and exercise their right to receive compensation.

Commentators disapprove of the NDPR's approach to penalties for violations of data subjects' rights. For instance, Olumide Babalola argues that the penalties under the Regulation only serve to generate income for the government at the expense of the actual victims of the

[113] *See* Regulation (EU) 2016/679, *supra* n 63, at Article 77(2).
[114] *Ibid*, at Article 79.
[115] *Ibid*, at Article 82.
[116] Nigeria Data Protection Regulation 2019, section 3.1(2).
[117] Regulation (EU) 2016/679, *supra* n 63, at Article 80.

breaches – the data subjects.[118] He also asserts that the NDPR should follow the GDPR's lead in adopting a right to compensation receivable by any person who suffered "material or non-material loss" as a result of infringement under the Regulation.[119]

Based off the differences between the GDPR and the NDPR discussed in this sub-section, problems with the NDPR include the failure to provide greater protection for sensitive data, including criminal conviction records; provide a strong framework for accountability, especially through imposing requirements for compliance reporting and disclosure of high-risk data breaches; and provide civil remedies for data subjects. Consequently, in some respects, the Regulation falls short in meeting its fourth objective – to ensure Nigerian business remain competitive in international trade. This objective is to be achieved through providing Nigerian businesses with a local regulation comparable to the GDPR. The gaps in the NDPR are particularly an issue here as it relates to the absence of higher protections for sensitive data, including financial records, and the absence of civil remedies for data subjects in Nigeria. Recall that for international data transfers, the GDPR requires the availability of appropriate safeguards and effective legal remedies that protect data subjects' rights in the destination country. Without higher protections for sensitive data and access to civil remedies for data subjects, Nigeria-based businesses may find it difficult transmitting personal data from the EU to Nigeria.

5.0. THE DPB IN COMPARISON TO THE NDPR AND GDPR

5.1. DPB Material Scope and Handling of Sensitive Data

The DPB covers data stored, collected, and processed by non-automated means,[120] thus responding to a significant gap in the NDPR, which only covers computerized data. The Bill also provides special protections for sensitive data.[121] However, unlike the GDPR, the Bill

[118] *Supra* n 68.
[119] *Ibid.*
[120] Nigeria Data Protection Bill 2020, Part I, section 2.1(a).
[121] *Ibid*, see generally Part VI.

still does not expressly provide special, or any, protections for criminal conviction records.

5.2. International Data Transfers (DPB)

The DPB is more protective of data subjects than the NDPR, keeping considerations for international transfers limited to the interests of data subjects or the public interest. According to the DPB, transfer of personal data is permissible where the data subject "has given explicit, specific and free consent, after being informed of risks arising in the absence of appropriate safeguards; or where it is in the interest of the data subjects; or if it is in line with public interest."[122]

Additionally, following the GDPR's lead, the DPB describes appropriate safeguards for the international transfer of data. These safeguards include those that are standardized and provided by legally binding and enforceable instruments adopted and implemented by the data controllers or data processors involved in the transfer and processing.[123] However, different from the GDPR, the DPB does not condition permissibility of data transfers on effective legal remedies being available to data subjects.

5.3. Data Processing Records (DPB)

Like the GDPR and unlike the NDPR, the DPB will require data processors and controllers to maintain records of their processing activities.[124]

5.4. Data Security and Data Breaches (DPB)

The DPB augments the NDPR in requiring data processors and controllers to notify data subjects and the Commission (set up under the Bill to regulate data processing activities)[125] of data breaches. The Bill requires data subjects to be notified of breaches within 48 hours of notifying the Commission.[126] However, unlike the GDPR, the DPB

[122] *Ibid*, at Part X, section 43.3.
[123] *Ibid*, at Part X, section 43.2(c).
[124] *Ibid*, at Part VII, section 32.4.
[125] *Ibid*, see generally Part III.
[126] *Ibid*, at Part V, section 17.3.

does not stipulate the timeframe for notifying the Commission of any breach.

5.5. Accountability (DPB)

5.5.1. Impact Assessment on Data Protection

Similar to the GDPR, the DPB requires DPIAs. Data controllers and processors are expected to regularly test, assess, and evaluate the effectiveness of their measures for ensuring the security of the processing.[127] Additionally, data controllers are obligated to take into consideration the risks arising from the interests, rights, and fundamental freedoms of data subjects, according to the nature, volume, scope and purpose of processing the data.[128] Data processors are also required to inform the data controller of any legal requirement that may create risks to the rights and fundamental freedoms of the data subjects, and to put into place measures to facilitate the data controller's obligations.[129]

5.5.2. Provision of Data Controller Representative in Country

Like the NDPR, the DPB still does not require data processors and controllers to have representatives on issues related to data processing in Nigeria.

5.5.3. Independence of Supervisory Authority

Similar to the NDPR, the DBP still does not provide for an independent supervisory authority. While a newly created commission replaces the NITDA, an agency of the Federal Government, as the supervisory authority to ensure compliance with the Bill,[130] the Commission is still overrun with Federal Government officials. 11 of the 16 members of the governing board of the Commission are Federal Government representatives, who would simultaneously be occupying their Federal Government positions while serving on the

[127] *Ibid*, at Part VIII, section 34.3.
[128] *Ibid*, at Part VII, section 30.1(c).
[129] *Ibid*, at Part VII, section 31.1(d).
[130] *Ibid*, at Part III, section 9(e).

Board.[131] The inclusion of government officials on the Board conflicts with the goal of strengthening Nigeria's legal institution through the DPB in order to allow for the Nigerian government to store and process citizen's data under a National ID system, without fears of data privacy violations.[132] In this respect, the DPB differs from the GDPR.[133]

5.6. Children's Data (DPB)

Compared to the NDPR, and in a similar fashion to the GDPR, the DPB provides additional requirements for the protection of children's data. The Bill expressly classifies children's personal information as sensitive data,[134] and requires data controllers to obtain the prior consent of the parent or guardian of a child before processing their data.[135]

However, different from the GDPR, the DPB does not require data controllers to make reasonable efforts to verify that consent has been given or authorized by the parent or guardian.

5.7. Remedies (DPB)

In line with the GDPR, the DPB provides civil remedies for data subjects. Particularly, it allows data subjects, either individually or through the Commission, to seek compensation or restitution through civil action for violations of their rights.[136]

However, like the NDPR, the DPB does not expressly require the Commission to inform data subjects about the progress and outcome of their complaints regarding violations of their rights; or of the possibility for judicial remedy. The DPB also does not give data subjects the right to representation by a not-for-profit organisation.

---

[131] *Ibid*, at Part III, section 8(1).
[132] *Supra* n 42.
[133] Recall that the GDPR prohibits members of each supervisory authority in States to refrain from occupying occupation incompatible with their duties. *See* Regulation (EU) 2016/679, *supra* n 63, at Article 52(4).
[134] Nigeria Data Protection Bill 2020, Part XIV, section 66.
[135] *Ibid*, at Part VI, section 26.2(b).
[136] *Ibid*, at Part XI, section 50.2.

In sum, if the DPB were to be enacted, it would tighten Nigeria's data protection regulatory framework, moving it closer in similarity to the GDPR. First, the DPB fixes the problems with the material scope of the NDPR, as protected personal data would include data stored in non-automated filing systems. Second, when it comes to international transfers, the Bill adopts language and safeguard requirements that are more protective of data subjects' rights. Third, the DPB requires covered entities to maintain records of their processing activities. Fourth, the Bill requires covered entities to notify the Commission and data subjects of data breaches. Fifth, the Bill will require covered entities to assess the effectiveness of their measures to ensure data security. Sixth, it classifies Children's data as sensitive data. Seventh, the Bill provides for civil remedies for data subjects and provides sensitive data with special protections. This seventh point is important, even as it would help streamline Nigerian businesses' ability to get approvals for personal data transfers from the EU to Nigeria, where there is business need.

However, the DPB still lags behind the GDPR in some respects. First, the Bill does not expressly include special protection for criminal conviction records. Second, the Bill does not require legal remedies to be available for data subjects in the destination country in the event of an international transfer. Third, the DPB does not specify a timeframe for notifying the Commission of data breaches, and consequently does not set a definite timeframe for notifying data subjects of a breach. Fourth, the Bill still does not require covered entities to have their representatives in Nigeria to promote accountability. Fifth, the Bill does not require controllers to make efforts to verify parental or guardian consent for processing of children's data. Sixth, the Bill does not provide for a completely independent supervisory authority. Lastly, the Bill does not require the supervisory authority to inform the complainant about the progress and outcome of their complaints, neither does it allow for not-for-profit representations of data subjects in cases of alleged violations.

6.0. POTENTIAL JUSTIFICATIONS FOR THE GAPS IN NIGERIA'S DATA PROTECTION REGIME

Once one takes the GDPR as a normative baseline and sees the NDPR, and soon to be enacted DPB, falling short as described, the next questions to answer are whether the Nigerian government has legitimate reasons for adopting a less stringent regulatory framework when compared to the GDPR, and what the practical implications of the chosen data protection regime are. To answer these questions, in this section, this writer assesses the ways the GDPR, through its extraterritorial effect, applies to many businesses in Nigeria. Keeping in mind that the extraterritorial effect of the GDPR does not apply to all institutions in the country, this writer examines other possible justifications for some outstanding gaps in the DPB. To do this, this writer highlights potential socio-economic justifications for Nigeria's data protection regime. This writer also explains ways in which the private sector is bridging some gaps left in the DPB.

At each stage of the discussion, despite the potential justifications offered, this writer finds that there remain persistent problems with Nigeria's regulatory framework that need to be addressed through amendments to the DPB. These issues are: the non-independence of the supervisory authority; difficulties in data subjects' access to remedies; and the absence of regulatory restrictions for public access to criminal conviction records.

7.0. THE EXTRATERRITORIAL EFFECT OF THE GDPR AS A POSSIBLE JUSTIFICATION FOR NIGERIA'S LOOSER REGULATORY REGIME

One of the reasons that the Nigerian government may have adopted a less stringent framework compared to the GDPR is due to the EU Regulation's extraterritorial effect. The GDPR affects companies either established or processing data in the EU. This means that many international businesses active in Nigeria, including the Big 4 – Amazon, Apple, Facebook, and Microsoft – must comply with the GDPR's data privacy compliance standards due to technical non-

divisibility.[137] However, the GDPR's extraterritorial effect does not completely resolve the problems with Nigeria's data protection regime. The Nigerian government and many local businesses fall outside the scope of GDPR, and thus are governed by Nigeria's local regulations – the NDPR and, if enacted, the DPB. The GDPR's extraterritorial effect also still does not resolve issues surrounding Nigerians' access to remedies for violations of their data rights within the country.

Through Article 3 of the GDPR, foreign entities (data processors and controllers) that do business in the EU are required to comply with the Regulation. The GDPR stipulates that the Regulation "applies to the processing of personal data by a controller or processor not established in the Union, but in a place where Member State law applies by virtue of public international law."[138] Covered processing activities include offering goods or services to, or monitoring, individuals located in the EU.[139] This means that businesses in non-EU states whose scope of operations fall within the provisions of Article 3 of the GDPR will have to comply with the Regulation to avoid facing penalties.

The GDPR also applies to the processing of personal data in the context of the activities of an *establishment* of a controller or a processor in the Union, whether processing activities take place in the Union.[140] According to the GDPR recitals, *establishment* "implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect." The implication being that once an organization is deemed an establishment, according to the criteria set forth in the recitals, the GDPR applies to its operations even though data processing is not taking place in the EU. The definition of establishment is consistent with Article 4(1)(a) of Directive 95/46.[141] The Court of Justice of the

[137] For a definition of "technical non-divisibility," see *supra* n 61.
[138] See Regulation (EU) 2016/679, *supra* n 63, at Article 3(2).
[139] *Ibid*, at Article 3(2)(a)(b).
[140] *Ibid*, at Article 3(1).
[141] Wiley, "The GDPR's Reach: Material and Territorial Scope under Articles 2 and 3", available at https://www.wiley.law/newsletter-May_2017_PIF-The_GDPRs_Reach-

European Union (CJEU) has interpreted what it means to be "established" under Directive 95/46 in two landmark cases – *Weltimmo* v *NAIH* (C-230/14) and *Google Spain SL, Google Inc.* v *AEPD, Mario Costeja Gonzalez* (C- 131/12).[142] In *Weltimmo*, the court held that in order to establish whether a data controller has an establishment in an EU Member State other than a third country where the controller company is registered, both the "degree of stability of the arrangements and the effective exercise of activities in that other Member State must be interpreted in the light of the specific nature of the economic activities and the provision of services concerned," especially for services offered exclusively over the internet.[143] The court further held that the presence of only one representative can, in some circumstances, suffice to constitute a stable arrangement if that representative acts with a sufficient degree of stability through the presence of the necessary equipment for provision of the specific services concerned in the Member State in question.[144] In this case, the court thus ruled that for the purposes of data processing that, Weltimmo, a company registered in Slovakia was established in Hungary, the EU, because Weltimmo runs one or several property dealing websites concerning properties situated in Hungary, which are written in Hungarian and whose advertisements are subject to a fee after a period of one month. Similarly, in *Gonzalez*, the court ruled that Google was established in Spain, the EU, because the data processing at issue in that case was related to the search business which Google Spain's sale of online advertising helped finance.[145] The decisions in the *Weltinmo* and *Gonzalez* cases apply to the GDPR due to the similarity in language with the Directive 95/46.[146]

With globalization, the wide-spreading reach of the internet, and the size of the EU market, in the bid to increase profits, both Nigerian

---

Material_and_Territorial_Scope_Under_Articles_2_and_3 (accessed 3 February 2021).

[142] *Ibid*.

[143] C-230/14, *Weltimmo* v *NAIH*, CURIA 29 (2015).

[144] *Ibid*, at p. 30.

[145] C-131/12, *Google Spain SL, Google Inc.* v *AEPD, Mario Costeja Gonzalez*, EUR-Lex 56 (2014); *see also* Wiley, *supra* n 141.

[146] *Supra* n 141.

businesses[147] and large foreign businesses[148] operating in Nigeria have exposed themselves to advertising their businesses within the EU and catering to EU residents. This means that they can easily be deemed established in the EU for the purposes of the GDPR. Thus, most businesses opt to follow the Regulation for all their data processing activities, especially due to the non-divisibility of data.[149] In fact, an analysis by Veritas Technologies, an information management company, suggests that 86 percent of organizations worldwide are concerned that a failure to adhere to GDPR could have a major negative impact on their business.[150] Nearly 20 percent of these businesses also fear that non-compliance could put them out of business.[151] This fear is warranted especially because of the large fines associated with violations of the GDPR. The foregoing illustrates the *Brussels effect:*[152] The EU's market size has attracted many companies, which process consumer data, to do business within the Union. The EU's strict data privacy regulations, which have extraterritorial effect, have caused many businesses to choose to adhere to the EU's regulations, especially due to the difficulty of separating their data services across multiple markets for technological reasons.

With most private data processors and controllers covered by the GDPR through the extra-territorial effect, the entities not affected by the GDPR's overhang tend to be smaller or more territorial (e.g., the Nigerian government). However, their data processing operations, especially that of the government, are large enough to pose real privacy risks to Nigerian citizens.

---

[147] Y. Kazeem, "African Startups Are Making the Risky Bet of Expanding beyond the Continent for Growth and Profits", available at https://qz.com/africa/1732046/swvl-lidya-paga-expand-from-africa-to-europe-asia-and-americas/ (accessed 3 February 2021).
[148] *Supra* n 47, at p. 28.
[149] *Ibid*, at p. 57.
[150] A. Bridgwater, "Worldwide Climate of Fear over GDPR Data Compliance Claims Veritas Study", available at https://www.forbes.com/sites/adrianbridgwater/2017/04/25/worldwide-climate-of-fear-over-gdpr-data-compliance-claims-veritas-study/?sh=7cd027ea680c (accessed 3 February 2021).
[151] *Ibid*.
[152] See Part II of this Paper.

When it comes to the government, what becomes most worrisome is (i) the lack of complete independence of the supervisory authority (NITDA, in the case of the NDPR, or the Commission, in the case of the DPB) from the Nigerian government; and (ii) assuming the DPB is enacted, complainants' ability to track their claims and attain not-for-profit representation. Without complete independence, there remains uncertainty about whether rights of data subjects will be fairly upheld when complaints against the government's data processing activities arise. This issue is particularly important due to the Nigerian government's history of oppressive acts against its citizens, including unlawful infringement on privacy rights.[153] There is no dispute that the NDPR should be supplemented with the DPB. However, given the limitations to the GDPR's extraterritorial effect, some amendments to the DPB are needed to enhance government accountability in data processing. First, like the GDPR, the Commission should be granted *complete independence* from the Federal Government and members of the Commission should not be permitted to hold positions within the government during their tenure. Also, it should be expressly stated that any decision by the President to oust the Data Protection Commissioner prior to completion of the Commissioner's tenure should be subject to review by the House of Representatives.[154] These

[153] According to the United States' Department of State in 2019, "significant human rights issues [in Nigeria] included unlawful and arbitrary killings, including extrajudicial killings, forced disappearances, torture, and arbitrary detention, all the above by both government and nonstate actors; harsh and life-threatening prison conditions; unlawful infringement on citizens' privacy rights; criminal libel; violence against and unjustified arrests of journalists; substantial interference with the rights of peaceful assembly and freedom of association in particular for lesbian, gay, bisexual, transgender, and intersex (LGBTI) persons and religious minorities; widespread and pervasive corruption; crimes involving violence targeting LGBTI persons; criminalization of same-sex sexual conduct between adults; and forced and bonded labor." *See* United States Department of State, Bureau of Democracy, H.R. and Lab., *2019 Country Reports on Human Rights Practices: Nigeria* 1 (2019); The government also recently tracked and clamped down on protesters against the Nigerian police brutality, even though they were exercising their constitutional right. *See* Vanguard, "#EndSARS Advocates Clamp Down: Descent into Tyranny – NAS", available at https://www.vanguardngr.com/2020/11/endsars-advocates-clamp-down-descent-into-tyranny-nas/ (accessed 3 February 2021).

[154] This amendment is necessary because of the Presidency's tendency to abuse its discretion in making such decisions. For instance, *see* The Associated Press, "Nigeria's Leader Suspends Chief Justice 3 Weeks before Vote", available at

changes to the DPB should be made in order to make the Commission less partial or fearful in conducting government-facing investigations. Another set of amendments that need to be made to the DPB involve expressly providing data subjects with the right to track the progress of complaints filed with the Commission. This will help data subjects ensure that their cases are being reviewed and investigated. Additionally, in the case of direct civil actions that data subjects bring, it would be prudent to follow the lead of the GDPR and allow for data-subject representation by non-profits. This is important because with the high poverty rate[155] and broken education system[156] in the country, many Nigerians cannot afford good lawyers and have limited knowledges of their rights.[157] They would thus benefit from external support from seasoned data protection NGOs.

7.1. Potential Socio-Economic Justifications for Nigeria's Data Protection Regime

As discussed, more territorial and smaller businesses tend to fall outside the GDPR's extraterritorial scope. Yet, the DPB leaves some substantial gaps in the NDPR unresolved. A look at Nigeria's socio-economic health and developing country status may justify the NITDA's decision to reduce some compliance burdens for businesses and, to a lesser extent, may justify placing criminal conviction records outside the scope of the DPB's protection.

---

https://www.nytimes.com/2019/01/25/world/nigerias-leader-suspends-chief-justice-3-weeks-before-vote.html (accessed 3 February 2021).

[155] According to the World Bank, 83 million people in Nigeria live in abject poverty. *See* World Bank, "The World Bank in Nigeria", available at https://www.worldbank.org/en/country/nigeria/overview (accessed 3 February 2021).

[156] S. Kehinde, "Nigeria's Public School System, A Blow", available at https://guardian.ng/opinion/nigerias-public-school-system-a-blow/ (accessed 3 February 2021).

[157] According to the United Nations Office on Drugs and Crime (UNODC), "[t]he financial limitation for qualification for legal aid is set at . . .5,000 naira per month (or US$ 43) in Nigeria, which still leaves quite a sizeable proportion of the population who earn more than 5,000 naira but are still unable to pay for private counsel uncovered." *See* UNODC, "Access to Legal Aid in Criminal Justice Systems in Africa Survey Report" 20 (2011), available at https://www.un.org/ruleoflaw/files/Survey_Report_on_Access_to_Legal_Aid_in_Africa.pdf (accessed 3 February 2021).

7.1.1. Nigeria's Framework may be an Attempt to Foster Economic Development.

Wealthier developed countries can better afford pursuing consumer protection at the expense of the profitability of their firms. However, for Nigeria, a developing economy, having less stringent regulatory standards for consumer data protection may be necessary to promote domestic enterprise development. In the world today, the ability of companies to collect, analyse, sell, and monetise user data with minimal restrictions is the basis for innovation and business growth; consumers are drawn by services targeted to benefit them and companies profit from the personal data collected from consumers.[158] Imposing stringent regulations on local businesses in a developing country restricts firms' ability to profit from analysing consumer data. Also, each additional obligation for businesses to comply with is likely to increase their cost of production. For instance, mandating that business find ways to confirm parental consent for children's data and setting hard deadlines for breach notifications, as in the DPB, will require more financial resources from local businesses that they may not have. Requiring data processors to have representatives within the country may also disincentivise foreign direct investment due to the increased cost of doing business. Furthermore, from the government's standpoint, enforcing a stringent regulatory regime will increase its financial costs.[159] Given that Nigeria is currently undergoing a recession, the country is unlikely to effectively manage a costly regime.[160]

Thus, Nigeria, a developing country pursuing economic growth, must strike the right balance between protecting consumer data and promoting domestic enterprise development. Femi Daniels, one of the

[158] B. Chakravorti, "Why the Rest of the World Can't Free Ride on Europe's GDPR Rules", available at https://hbr.org/2018/04/why-the-rest-of-world-cant-free-ride-on-europes-gdpr-rules (accessed 3 February 2021).

[159] *See* United Nations Conference on Trade and Development (UNCTAD), "Data Protection Regulations and International Data Flows: Implications for Trade and Development" (2016), available at https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf (accessed 3 February 2021).

[160] N. Munshi, "Nigeria Slumps Back into Recession as COVID Bites", available at https://www.ft.com/content/ea70f0b4-5f13-423b-b1ed-6d6c424d1b91 (accessed 3 February 2021).

drafters of the NDPR, also makes this argument in brief.[161] In defending the looser regulations in the NDPR compared to the GDPR, Daniels points to the need to seek balance between "a strict data protection regulatory regime and economic opportunities emanating from relaxed data protection regimes."[162] He says, "it is . . . unrealistic and inhibitive of desperately needed foreign investment and opportunities, for Nigeria to aim too high with respect to their regulations."

7.1.2. Nigeria's Framework may be an Attempt to Lower Crime Rates

The decision not to place criminal conviction records under the protection of either the NDPR or the DPB may be a purposeful move amidst the impending enactment of the Crime and Criminal Tracking System Bill (2019).[163] This Bill will require the design, development, installation, and management of a crime and criminal tracking database for the Nigerian police with the purpose of enhancing national security.[164] It will require all available criminal history for a person to be available online, and this information will be available to the general public.

The need to clamp down on crime rates in Nigeria is indeed urgent.[165] However, this need should not completely overrun the need for some forms of restrictions to the public in accessing individuals' criminal

---

[161] Kirpatrick, *supra* n 9.
[162] *Supra* n 45.
[163] U. Chiefe, "Nigeria is Planning a Digital Criminal Registry; You Should Probably Be Worried", available at https://techpoint.africa/2019/10/09/criminal-bill-nigeria-trust-privacy-corruption/(accessed 3 February 2021).
[164] *Ibid*.
[165] According to the United States Department of State, "Crime is prevalent throughout Nigeria. Most crime directed toward U.S. travellers and private-sector entities in southern Nigeria seeks financial gain. U.S. visitors and residents have been victims of a wide range of violent crime, including armed robbery, assault, burglary, carjacking, rape, kidnapping, and extortion. The mostly commonly reported crimes are armed robbery, kidnap for ransom, and fraud. In addition, mainland portion of Lagos has experienced periodic outbreaks of violence, resulting from clashes among localized street gangs known as 'Area Boys.'" *See* United States Department of State, "Nigeria 2019 Crime & Safety Report: Lagos", available at https://www.osac.gov/Content/Report/4a5eaf52-3655-43e6-b540-1684bcb6f3de (accessed 3 February 2021).

conviction history. This is especially due to the broken police[166] and judiciary[167] systems in Nigeria, as well as the high rate of wrongful convictions for crimes.[168] Additionally, with the life-shattering consequences of criminal records to a person's employability and social standing, there needs to be some privacy restrictions on access to these records. Perhaps to account for the higher crime rates in Nigeria compared to the EU, legislators should adopt a less stringent variation of the GDPR's standards for the protection of criminal conviction records. In any case, this issue of striking the right balance between data protection and national security ought to remain in sharp focus with appropriate deliberation by legislators and civil society at large.

7.2. The Role of the Private Sector in Addressing Some of the Limitations to Nigeria's Looser Regulatory Framework

The GDPR's extraterritorial effect does not also resolve issues concerning the accountability of all data processing entities in Nigeria to the NITDA or the Commission, particularly as it relates to data breach reporting. As already discussed, while the DPB augments the NDPR in requiring data breach reporting, unlike the GDPR the Bill does not give a timeframe for making these reports. A potential reason for leaving this issue unaddressed in the DPB may be due to the role of the private sector in improving cybersecurity. Note that cybersecurity is a necessary complement to data processing regulations because the latter limits opportunities for institutional

[166] J. Campbell, "Nigerian Police are in Desperate Need of Reform", available at https://www.cfr.org/blog/nigerian-police-are-desperate-need-reform (accessed 3 February 2021).

[167] T. Osasona, "Time to Mend Nigeria's Broken Criminal Justice System", available at https://guardian.ng/features/youthspeak/time-to-mend-nigerias-broken-criminal-justice-system-1/ (accessed 3 February 2021); *see also* Y. Kazeem, "Up to Three-Quarters of Nigeria's Prison Population is Serving Time Without Being Sentenced", available at https://qz.com/africa/892498/up-to-three-quarters-of-nigerias-prison-population-is-serving-time-without-being-sentenced/ (accessed 3 February 2021).

[168] D. Ehighalua, "Nigerian Issues in Wrongful Convictions" (2013) 80(4) *University of Cincinnati Law Review*, p. 1131.

misuse or abuse of personal data, and the former prevents external hackers from fraudulently accessing personal data.

The underlying challenge with the absence of a reporting timeframe in Nigeria's data protection regime is that the Commission may be slower or unable to review and process data breach reports. As previously discussed, reporting breaches to the supervisory authority may play an important role in enhancing cybersecurity.[169] This is because information from data breach reports can be analysed and disseminated in the bid to fortify companies' security protocols.

For the Nigerian government, allowing the private sector to combat data breaches may be more effective than putting its limited resources towards tightly tracking, analysing, and disseminating data breach reports to improve cybersecurity. This is because the private sector in Nigeria possesses larger technological and budget capacities than the public sector, making it a more efficient provider of cybersecurity services.[170] A look at recent developments amongst Nigeria-based businesses confirms this theory: With the assistance of private security companies, businesses in Nigeria are gearing up to defend themselves against cybersecurity breaches.

Assisted by privately owned security operation centres, companies are implementing protective and security monitoring mechanisms and increasingly subscribing to cyber insurance to defend against breaches. Knowledge of the modes through which data breach occur is also spreading across businesses not just in the financial sector – Nigeria's tightest regulated sector – and they are already taking action and

[169] *See* Part II of this Paper.

[170] The public sector works with a tighter budget and possesses limited technological capacities. *See* A. Estache and L. Wren-Lewis, "Toward a Theory of Regulation for Developing Countries: Following Jean-Jacques Laffon's Lead" (2009) 47(3) *Journal of Economic Literature*, pp. 729 and 733 (discussing the limited regulatory capacity of developing countries: "Regulators are generally short of resources, usually because of a shortage of government revenue and sometimes because funding is deliberately withheld by the government as a means of undermining the agency. The lack of resources prevents regulators from employing suitably skilled staff, a task that is made even harder by the scarcity of highly educated professionals and the widespread requirement to use civil service pay scales. Beyond the regulator itself, an underdeveloped auditing system and inexperienced judiciary further limits implementation".

expected to take more action to ensure security of data. The Deloitte Nigeria Cyber Security Outlook 2020 reports that in 2019, organizations in Nigeria took strategic decisions by implementing or subscribing to Security Operation Centres to monitor and defend their firms from existing and emerging threats.[171] Consequently, there was a rise in cyber threat monitoring services which has helped many organizations secure their most priced data. The increases in cybersecurity consciousness across organizations in Nigeria has also led to increased success in detecting and responding to cyber-attacks and breaches within the shortest possible times.[172] Cyberthreat monitoring and intelligence services in Nigeria have also been projected to transition from manual monitoring techniques to reliance on AI and machine learning monitoring to help uncover attacks before they happen, and ultimately gain an advantage against fraudsters and hackers.[173] There is also projected to be an increase in organizations in Nigeria exploring cyber insurance as against focusing efforts solely on preventive measures for detecting and blocking potential attacks as well as practices around disaster recovery to enable an appropriate response.[174]

The GDPR's extraterritorial effect, Nigeria's socio-economic climate, and private sector cybersecurity activities may justify the looser regulatory regime in Nigeria. However, they are not full-proof vindications for certain persistent gaps in the NDPR and DPB, namely; the non-independence of the supervisory authority; difficulties in data subjects' access to remedies; and the absence of regulatory restrictions for public access to criminal conviction records. Changes must be made to the DPB, to correct for these deficiencies.

8.0. CONCLUSION

The enactment of the NDPR in 2019, which followed the passage of the GDPR into law in 2016, represented a glimmer of hope for the proper protection of data subjects' rights in Nigeria. However, with

[171] T. Aladenusi, "Nigeria Cyber Security Outlook 2020", available at https://www2.deloitte.com/ng/en/pages/risk/articles/nigeria-cyber-security-outlook-2020.html (accessed 3 February 2021).
[172] *Ibid*.
[173] *Ibid*.
[174] *Ibid*.

its deviations from the GDPR in areas that importantly protect individual's constitutional privacy rights and hold businesses properly accountable for their data processing actions, the DPB needed to be introduced to strengthen the legal institutional framework for data protection in Nigeria. This is especially true as Nigeria seeks to execute a Data Identification for Development Project that will leave most Nigerian's personal data at the mercy of the government. While the Data Protection Bill provides more protection for personal data than the NDPR, it still has certain gaps that need to be addressed. Yes, the GDPR and private sector are a good supplement to Nigeria's regulatory system, and yes, Nigeria's status as a developing economy warrants a looser regulatory framework. However, certain aspects of the DPB remain problematic. These include: the non-independence of the supervisory authority, difficulties associated with data subjects' access to remedies, and the absence of regulatory protections for criminal conviction records. Legislative advocates must seek to have these issues with the DPB corrected to make it a viable supplement to the NDPR. Most importantly, from a broader perspective, it should be emphasized that there needs to be an institutional commitment to the enforcement of the NDPR and DPB, if enacted, if not the data privacy regulations in the country will have no teeth.