LAGOS
BUSINESS
SCHOOL

PAN-ATLANTIC UNIVERSITY

Data Protection in Nigeria White Paper

April 2022

EXECUTIVE SUMMARY

The fourth industrial revolution (4IR) and emergent information and communication technologies (ICTs) are speeding up Nigeria's digital transformation. An economy in transition requires synergies between the digital, legal, political and socio-economic infrastructures to realise the benefits and curb attendant risks of the digital economy. Thus, as we embrace digital technologies, mindfulness about social policies like data protection and privacy policies are critical to maintaining citizens' human rights in an online world. The increased risks of ICTs warrant regulatory changes around the world, especially as it relates to data and privacy. In 2016, the European Union (EU) introduced the General Data Protection Regulation (GDPR) providing guidance on the governance and control of personal data. This trailblazing legislation adopts core principles like openness, data security and purpose specification, accountability and data quality, leaving member States to implement liberally.

In Nigeria, Other than the Constitution that conveys Nigerians the right to privacy, we lack a holistic legal and policy framework for data protection. Several efforts to legislate data protection have been unsuccessful and sectoral regulators and the National Information Technology Development Agency (NITDA) are bridging the gap. This white paper argues that as we embark on a national digital transformation journey, adopting diverse digital technologies, there will be significant privacy risks, warranting effective policies and regulations to govern and control data. The paper reviews the 2020 bill alongside global benchmarks, with recommendations regarding:

Sale of personal data: the bill only prohibits the sale where a person receives or discloses personal data to a third party intentionally or recklessly without the consent of the data controller, or after acquiring personal data, keeps it without the consent of the data controller. Therefore, permitting the sale of personal data monitoring such sales will be difficult and can cause abuse.

Treatment of artificial legal persons: the bill seems to be limited to protecting data of natural persons, breach of data of artificial entities may prove detrimental to the persons in such organizations and even the business itself. Hence, the bill should be more inclusive.

Interpretations: The bill does not include certain relevant terms in the interpretation section such as trans-border. Hence, the interpretation section of the bill needs to be expanded.

Third-party processing contracts: Unlike the NDPR which stipulates that a written contract should be made between the third party and the data controller, this bill merely provides that when a data processor hires a third party to meet its obligations to the data controller, the data processor must impose the same data protection obligations outlined in its contract with the data controller, and the data processor is liable to the data controller for ensuring the third party's obligations are met. Therefore, the bill should be amended to include an express provision for the contract.

Cloud Data Protection: The bill does not recognise the need for data protection in the cloud. Everyday, people upload their personal data such as financial information and other forms of

sensitive data to the cloud using software applications. While cloud solutions provide lower cost digitalization options for small businesses, protecting such data is essential. Thus, the bill should include data encryption provisions and data retention periods for cloud service providers. The service providers must understand and comply with the jurisdictional privacy requirements if they are to operate within the jurisdiction.

Role of Nigeria Data Protection Bureau and NITDA: Nigeria conceived the NDPR as an interim measure prior to substantive legislation. Given the slow progress, the President approved the establishment of The Nigeria Data Protection Bureau (NDPB) as the regulatory agency with the primary mandate of data protection and privacy in Nigeria. Without an enabling law, the full extent and scope of this body's power and duties are currently unclear, but it is reported that it merges the gains of the NDPR and will support the development of legislation for data protection and privacy. However, there can be a synergy between these regulatory agencies, mirroring the approach adopted with the Nigerian Code of Corporate Governance, 2018 and the Federal Competition and Consumer Protection Act, 2018.

Data Localization: To address these challenges and level the playing field, the provisions of data localization should be based on data sensitivity and risks. Such a data classification framework ensures the proper processing of sensitive data, reducing the risk of data privacy and protection.

Nigeria's economy is in transition and requires policies and regulations that will enable a conducive and enabling environment. The benefits of data protection are significant to Nigeria's economy as we seek to diversify and build a digital economy. Thus, a national, holistic and coordinated approach led by a single central regulator, working alongside other government ministries, departments and agencies (MDAs) is fundamental and reducing the administrative burden of sector-specific regulators.

LAGOS BUSINESS SCHOOL
PAN-ATLANTIC UNIVERSITY

CONTENTS

ABBREVIATIONS AND ACRONYMS

CCPA	California Consumer Privacy Act
DPA	Data Protection Authority
DPO	Data Protection Officer
DPCO	Data Protection Compliance Organization
EU	European Union
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
LGDP	Lei General de Proteção de Dados Pessoais (Brazilian version of GDPR)
MDA	Ministry, Department and Agency
MSME	Micro, Small and Medium Enterprise
NCC	Nigerian Communication Commission
NDPR	Nigerian Data Protection Regulation
NDPB	Nigeria Data Protection Bureau
NITDA	National Information Technology Development Agency
PID	Personal Identifiable Data
PII	Personal Identifiable Information
RAID	Redundant Array of Independent Disks

GLOSSARY OF TERMS

Term	Description
Anonymization	Rendering data into a form which does not identify individuals and where identification is not likely to take place.
Cloud Computing	Internet-based computing, providing shared computing resources, software and information and other devices on-demand.
Confidentiality	The duty not to share information with persons who are not qualified to receive that information.
Consent	Any freely given, specific, informed and unambiguous sign of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.
Data Controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data Processor/Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Data Protection Authority	An independent body which, amongst other things: • Monitor personal data processing within its jurisdiction (country, region or international organization); • Advise competent bodies regarding legislative and administrative measures relating to the processing of personal data; • Manage complaints lodged by citizens regarding the protection of their data protection rights.
Data Protection Compliance Organization (DPCO)	Independent entities licensed by NITDA to monitor, audit, conduct training and data protection compliance consulting to all Data Controllers as defined in the NDPR.
Data Protection Officer	A role within an entity that enables compliance with data protection legislation and fostering a data protection culture within the entity and helps implement essential elements of data protection legislation, such as: • Principles of data processing • Rights of data subjects • Data protection by design and by default • Records of processing activities • Security of processing • Notification and communication of data breaches
Data Subject	People – the natural persons whose personal data are processed

Term	Description
Digital Economy	An economy based on digital computing systems and synonymous with conducting business online.
Personal data	Any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as name, identification number, location data, online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personally identifiable information such as names or addresses. Public and non-sensitive information can also fall within the scope of 'personal data,' as do pseudonymous identifiers, IP addresses, tracking cookies, and similar data.
Privacy	The ability of an individual to be left alone, out of public view, and in control of information about oneself.
Processing	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means. Activities include collecting, storing, disclosing, and erasing data.
Pseudonymization	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
Sensitive Data	Special categories of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and genetic data, biometric data processed for the purpose of uniquely identifying a natural person, or data concerning health, a natural person's sex life or sexual orientation.

Introduction

The increased risks of information and communications technologies warrants rapid regulatory changes around the world especially as it relates to data and privacy. *The 2016 EU's General Data Protection Regulation (GDPR)*[1] has spurred increasing global interest in the governance and control of personal data. Many economies now have a strong interest in protecting the indiscriminate free flow of personal data[2]. Rising internet connectivity, broadband access and digitalization through technologies like cloud computing that coincide with broader inclusive development drives, have motivated many societies to form policies to govern the digital landscape. However, in many African nations', rules governing personal data protection are a patchwork[3] due in part to the gaps in the current governance of data protection and privacy[4].

Data includes facts, figures and information. It can be defined as individual units of information, measured, collected and reported; stored and analysed. Data covers *medical records, personal emails, personal information, criminal records, financial records, employment records, and other important information about individuals and corporations*, *either electronic or paper.* The European Data Protection Board defines data as the "gigantic digital datasets held by corporations, governments and other large organisations, which are then extensively analysed using computer algorithms"[5]. In this digital era, data is an organisational asset and the most valuable resource, which when properly analysed, improves decision making and business performance, making it attractive to businesses and governments. The world's most valuable listed corporations like Microsoft, Amazon, Apple, Facebook and Alphabet Inc (Google) use large quantum of data. Table 1 lists key attributes and characteristics of data.

Table 1: Data attributes and characteristics (Source: Authors' illustration)

Quality	**Attribute/Characteristic**	
Personal	Private	Public
	Identified	Pseudo Anonymised
Non-Personal	Anonymous	Machine data
Timeliness	Instant/Live	Historic

1 In 2016, the European Union enacted the EU Regulation 2017/679- also known as the EU GDPR to shape and regulate personal data in the EU.

2 Personal Data (also known as Personal Identifiable Data (Information) or PII/PID) are any information which are related to an identified or identifiable natural person (Art .4(1) of GDPR: https://gdpr-info.eu/issues/personal-data/)

3 Some other African nations (a handful, perhaps) have extensive digital governance frameworks. About ten countries have enacted some form of data protection legislation: Burkina Faso, Cabo Verde, Côte D'Ivoire, Ghana, Kenya, Kenya, Liberia, Malawi, Morocco, Nigeria, Senegal, Seychelles,, Sierra Leone, South Africa and Tunisia. Malawi and Nigeria have only draft legislation

4 Daigle, B. (2021). Data Protection Laws in Africa: A Pan-African Survey and Noted Trends. *J. Int'l Com. & Econ.*, 1.

5 De Hert, P., & Papakonstantinou, V. (2021). Framing big data in the council of Europe and the EU data protection law systems: Adding 'should' to 'must' via soft law to address more than only individual harms. *Computer Law & Security Review*, *40*, 105496.

Format	Structured	Unstructured

Data protection/security involves the set of strategies, policies and processes that ensure the privacy, availability and integrity of data. It helps to prevent data loss, theft, or corruption and can help mitigate the damage done in the event of a breach, disaster, or an unprecedented situation. Data protection and privacy are often used interchangeably; however, this is erroneous. The latter implies those with access to data, and the former provides the tools and policies to restrict access to the data. Data protection traverses three broad categories - traditional data protection (such as backup and restore copies), data security and data privacy - ensuring the security and protection of data while at rest and in transit (see Figure 1).

Figure 1: Data protection categories (source: Authors' illustration from Storage Networking Industry Association, 2022)

As more and more social and economic activities take place online, the United Nations Conference on Trade and Development (UNCTAD) in recognizing the importance of privacy and data protection identifies eight (8) core principles to guide member nations'[6] data protection legislations albeit with varying implementation practices that are discussed in subsequent sections. Some notable trends in data protection are iterated in subsequent paragraphs.

- **Data Graveyard and New Privacy Standards**: This term describes the repositories of unused data. Data graveyards exist because of varying retention and removal standards and could be perceived as stockpiling and increase the compliance burdens on storage/retention durations.
- **New Roles and Shifts in Responsibility:** Another cynosure in data privacy/protection is related to the shift in compliance responsibilities. Businesses must recognize that a single role (maybe of data protection officer) may be incapable of single-handedly managing, supervising and implementing data protection laws and regulations.

6 According to UNCTAD, 137 out of 194 countries had put in place-as at 2021- legislations to secure the protection of data and privacy.

- **More Penalties and More Awareness**: Managing data protection increases the administrative and compliance burdens of regulatory authorities and businesses respectively[7]. With such outcomes like fines and reputational damage, creating awareness amongst employees and a compliance culture are essential.
- **Transparency, Effectiveness and Trust:** the importance of these key governance ethos now and in the future cannot be over emphasised. With consumers being more aware of their rights, attitude towards transparency, privacy and trust are becoming more pronounced, forcing companies and governments to bring more attention to these issues.
- **Third Party Risk Management:** businesses must also manage the compliance of third-party exposure from suppliers, vendors, and other stakeholders. The case of Facebook's whistleblowing exposure[8] was on third party risk management, risk assessment and demands to comply.
- **Talent Crisis and Retraining and Retooling Employees/Orienting the public:** the developing nature of new technologies is introducing additional risks and challenges that mandate organisations implement strategies to build requisite expertise and continuously re-skill and re-tool employees and other stakeholders.

Globally, the increasing use of communications networks that facilitate data transmission within minutes and emerging technologies like social media and the Internet of Things (IoT)[9]that support the generation of large amounts of human and machine-oriented data, raise concerns about the protection and privacy of such data. With the increasing socio-politico-economic interactions, enacting legislation to protect PIDs cannot is important. Over the years, there have been attempts to conceal personal data of individuals through efforts like anonymisation, pseudonymization, encryption, key-coding, and data sharing. However, these efforts are not fool proof, and anonymized data can be re-identified and attributed to specific individuals.

The substantial increase in the internet's use on the African continent[10] is aided by the ongoing private and public investment in digital infrastructure, a significant reduction in associated costs and improved user access. This has allowed distinct entities to access, collect, process, use, and disseminate personal data more quickly. In Nigeria, there have been a worrisome amount of data

7 As at 2021, the total estimate of GDPR fine since inception for non-compliance was a paltry €275 million.

8 Haugen was

https://www.npr.org/2021/10/05/1043377310/facebook-whistleblower-frances-haugen-congress

9 Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., Li, J., & Poor, H. V. (2021). Federated learning for internet of things: A comprehensive survey. *IEEE Communications Surveys & Tutorials*.

10 More specifically, in Nigeria internet usage increased by 72,375% from 200,000 people in the fourth quarter of the year 2000 to 144,749,194 people as of the fourth quarter of 2021. Retrieved from Internet World Stats, Africa Internet Users, 2021 Population and Facebook Statistics (internetworldstats.com); Africa Internet User Stats and 2022 Population by Country (internetworldstats.com) accessed 27th March, 2022.

breaches over the past few years, as organisations now infringe on the privacy of Nigerians by using the information given to them for purposes other than what they were collected for. For instance, the Lagos State Internal Revenue Service (LIRS) published the personal information of taxpayers on their payment platform because of technical glitches[11]. These glitches are in breach of the Nigeria Data Protection Regulation (2019). Other instances of data privacy breaches include the case between the National Information Technology Development Agency (NITDA) and Truecaller in 2019 and MTN Nigeria Communications Limited and Barrister Godfrey Eneye in 2013[12].

There are growing concerns amongst African countries and Nigeria regarding protecting citizens' personal data, regulate public and private use of that data, and establish data protection agencies to enforce these legislations. This has spurred several African countries to enact comprehensive data protection legislation, while others have remained relatively slow in the enactment and adoption of data protection legislation, with Nigeria not an exception.

This white paper argues that as we embark on a national digital transformation journey, adopting diverse digital technologies, there will be significant privacy risks, warranting effective policies and regulations to govern and control data. The white paper introduces the tenets of data protection in Nigeria, against global best practices and proposes policy recommendations for legislative change. Following this introduction, we present an overview of best practices vis-à-vis Nigeria's regulations and regulatory attempts on data protection. We then present a cursory view of the data protection bill, identifying the implementation challenges. Next, we highlight similarities and differences between the Nigerian data protection bill and global best practices, provide a few case studies of some countries globally, and conclude with recommendations.

Global Best Practices

At the outset, it is instructive to note that the term data privacy is included in the broader concept of **'data protection'**[13]. Holistically, data privacy (or, *information privacy*) is a core part of data protection that concerns proper handling of sensitive data, including notably, personal data; but other discreet information such as certain financial data and intellectual property rights, to meet certain regulatory requirements and protecting the immutability, sensitivity and confidentiality of those data.

11 More information available at: Breach of Nigeria Data Protection Regulation by the Lagos State Internal Revenue Service (proshareng.com)

12Francis O. (2020). Data Privacy and Protection under the Nigerian Law. Available at: Data Privacy and Protection under the Nigerian Law – Francis Ololuo – S.P.A. Ajibade & Co. Resources (spaajibade.com)

13 For more on this , please see: https://www.snia.org/education/what-is-data-privacy#:~:text=Data%20privacy%2C%20sometimes%20also%20referred,meet%20regulatory%20requirements%20as%20well

Globally, privacy is a fundamental human right recognized by all major international treaties and agreements on human rights and in the constitutions of different countries, either explicitly or implicitly. Newly redrafted constitutions also include specific rights to access and control one's personal data/information. At the turn of the millennium, there was a global concerted effort to enact comprehensive and far-reaching privacy and data protection acts around the world either to address the perceived governmental abuses or to align standards and ensure compatibility with reputable international organisations[14].

The coming to fruition of GDPR marked a watershed moment in the data privacy era. The content is such that governments and policymakers have the incentive to revisit, re-regulate and redraft laws to create one cohesive national law. Setting the guiding light via the GDPR, the EU set a commendable example by creating a framework where organisations take responsibility for how they process, divulge, share, and store personal identifiable data (PID). The EU-GDPR framework has also shown flexibility and market inclusiveness. Albeit, a marathon, GDPR on other legislative systems globally cannot be overlooked[15]. Additional data privacy initiatives spurred by the GDPR include Brazils General Data Protection Law of 2020; Asian Data Privacy initiatives[16] and notably the Nigerian Data Protection Regulation (NDPR).

UNCTAD Principles

The United Nations Conference on Trade and Development (UNCTAD) highlights 8 core principles (see Figure 2[17]) to promote compliance about how personal data is collected, processed and used. These principles adhere to the international and regional agreements and guidelines and may vary in implementation practices. The principles are openness, collection limitation, purpose specification, use limitation, security, data quality, access and correction and accountability.

14 Banisar, D., & Davies, S. (1999). Global trends in privacy protection: An international survey of privacy, data protection, and surveillance laws and developments. *J. Marshall J. Computer & Info. L.*, *18*, 1.

15 One important act inspired by the GDPR is the California Consumer Protection Act (CCPA 2020) which was the first US privacy law of a similar magnitude. Please note that California is the fifth largest economy in the world. https://www.cbsnews.com/news/california-now-has-the-worlds-5th-largest-economy/

16 The Aisan versions are coming on strong as well with many initiatives mooted to create laws that will give the consumers a certain amount of control over their personal information.

17 United Nations Conference on Trade and Development. Data protection regulations and international data flows: Implications for trade and development. https://unctad.org/system/files/official-document/dtlstict2016d1_en.pdf (2016).

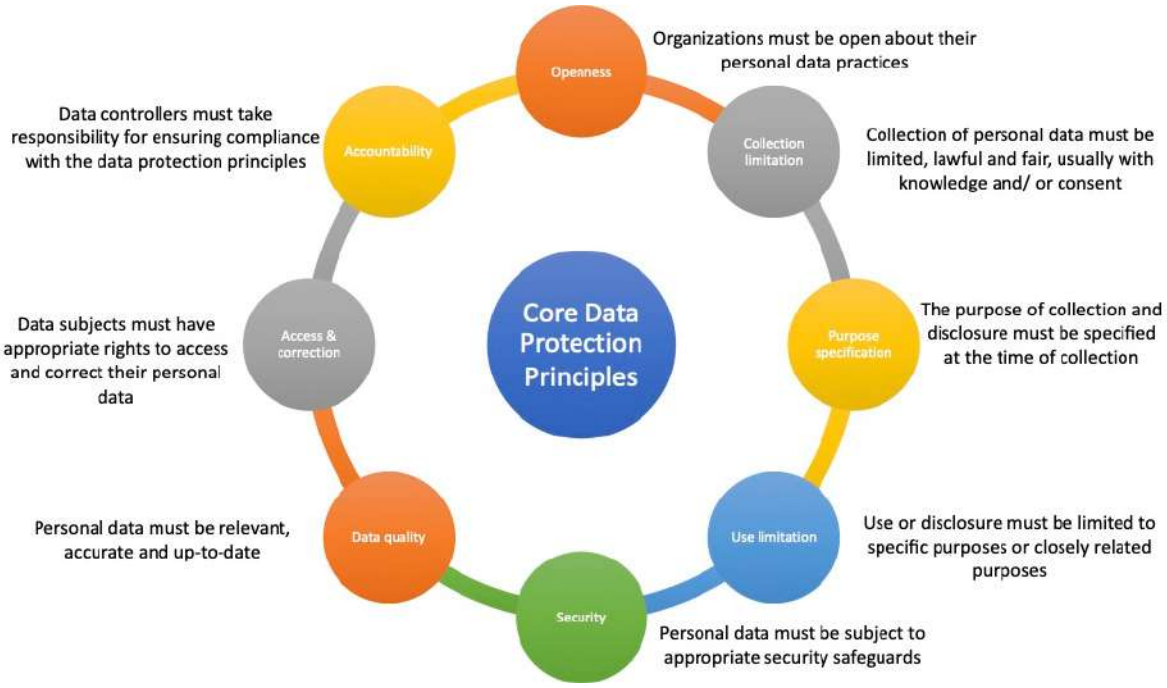

Figure 2: UNCTAD data protection principles (Source: Authors' illustration)

The principles address the treatment of personal data, expected behaviours of organisations, key responsibilities of data controllers and the rights of data subjects.

Data Privacy Regulations in Nigeria

The Constitution of the Federal Republic of Nigeria (as amended) serves as the foundational regulation for data protection in Nigeria. It describes the protection of personal data and information as a constitutional right. Several attempts have been made to protect personal information within the country. These attempts give more context and perspective to the constitutional provision. However, most of these laws on data protection are sector or industry specific. Figure 3 highlights the regulations and different key acts to protect personal information within Nigeria.

Figure 3: Regulations and data protection attempts (source: Authors' illustration)

Prior to introducing NDPR in 2019, the absence of governing data protection legislation covering the entire economy[18] resulted in sectoral practices by regulatory agencies. NDPR explains the provisions of the Constitution and shapes data protection in Nigeria covering natural persons who are citizens of Nigeria either at home or abroad. The regulation makes provision for the rights of data subjects, the responsibilities of data controllers and processors, data localization and guideline for the safekeeping of personal data among others.

Notwithstanding, attempts have been made at passing data protection bills in Nigeria. Two proposed bills have not successfully passed the required processes[19]. Another bill was proposed by an agency of the federal government but is yet to be presented before the national assembly.

A Cursory View of the Data Protection Bill (2020)

The data protection bill was borne out of the limitations of the NDPR in scope, form and power. It was drafted because of the need for a comprehensive law that solely governs data privacy and protection. The Data Protection Bill 2020 (the Bill) was introduced in March 2020 by the Federal

18 Francis O. (2020). Data Privacy and Protection under the Nigerian Law. Available at: Data Privacy and Protection under the Nigerian Law – Francis Ololuo – S.P.A. Ajibade & Co. Resources (spaajibade.com). Khadijah El-Usman (2021). A push toward data protection legislation in Nigeria. A. Accessed 30th March, 2022.

19 Khadijah El-Usman (2021). A push toward data protection legislation in Nigeria .A push toward data protection legislation in Nigeria - Paradigm Initiative (paradigmhq.org). Accessed 30th March, 2022.

Government through the Legal and Regulatory Reform Working Group (LWG) in furtherance of the Federal Government's implementation of the Nigeria Digital Identification for Development (ID4D) project[20].

Objectives and Scope of the Bill

The purpose of the bill is to establish an efficient regulatory framework for protecting personal data, regulate the processing of information relating to data subjects and to safeguard their fundamental rights and freedoms as guaranteed under the Constitution of the Federal Republic of Nigeria[21].

Scope of Application

The bill applies to the processing and use of personal data of both Nigerians and non-Nigerians living in Nigeria, by automated and non-automated means[22]. This means that the bill extends also to the processing of non-electronic and electronic data. The scope also extends to personal data processed by private and public organisations within the Nigerian state[23]. The bill also applies to data controllers and processors of personal data where they are both established in Nigeria, the personal data of the data subject is processed in Nigeria, or the data subject lives in or outside Nigeria. The bill will also apply where a data controller is not established in Nigeria but uses equipment or a data processor to process data of subjects that live in or outside Nigeria, or where processing is carried out regarding data subjects that live in or outside Nigeria and such data originates partly or wholly from Nigeria[24]. The bill states six categories of persons to be covered, including Nigerian citizens, Nigerian residents, organisations incorporated in Nigeria, unincorporated joint ventures or businesses operating in whole or partly in Nigeria, persons who operate an office, branch or agency through which business activities are carried out in Nigeria and foreign entities targeting Nigerian residents[25]. The bill also applies to certain types of personal data including biometric data, sensitive personal data, personal banking and accounting records, data that reveals a data subject's flight reservation, academic transcript records, and medical and health records[26]. It also provides that data controllers or processors are required to submit data protection audit reports to the Data Protection Commission annually and not later than 30th March. The NDPR also contains this requirement to submit audit reports, however, the NDPR requires only data controllers that process personal data of over 2000 data subjects to submit annually, not later than the 15th of March. The commission is required to

20 NIMC, Submit Comments on the Draft Data Protection Bill 2020, https://www.nimc.gov.ng/submit-comments-on-the-draft-data-protection-bill-2020/, accessed 2nd April 2022

21 Section 1 of the Data Protection Bill

22 Section 2(1)(a)

23 Section 2(1)(b)

24 Section 2(1)(c)(i)-(iv)

25 Section 2 (3)

26 Section 2 (4)

compile and publish a report containing the list of organisations that have submitted the audit report annually[27].

Basic Principles and Legal Basis for Processing Personal Data

The bill highlights personal data must be processed for specific and legitimate purposes and in a lawful, fair, transparent manner. These are the basic principles that a data controller or processor must comply with when processing personal data. These principles are also like those contained in the NDPR[28].

There are also provisions that show instances where the processing of personal data will be lawful. Personal data will be held to have been lawfully processed if it was processed for performing a contract, compliance with a legal obligation, protection of vital interests of a data subject or another person, or a prevailing legitimate interest pursued by the data controller or a third party[29]. However, the exception of an overriding interest will not apply when such is overridden by the interest of fundamental rights of the data subject.

Establishment, Composition, Power and Functions of the Data Protection Commission

The Bill established the Data Protection Commission and its Governing Body[30]. The governing board comprises relevant parties from the data privacy sector and government institutions that deal with substantial volumes of data. The Commission may effectively implement compliance with the terms of the Bill, make administrative arrangements that it deems suitable to discharge its duties, investigate complaints based on the Bill, make regulations, apply to the court for a warrant, impose fines and penalties, and carry out its duties with the support of enforcement agencies. The Commission is also mandated to develop rules for the licensing and certification of data protection compliance officers and organisations[31].

Rights of Data Subjects

The Bill establishes data subjects' rights, which are supplanted by the provisions of Section 38 of the proposed Act, which address the rights of anyone affected by the processing of any personal data to request from the Commission an evaluation of whether such processing conforms with the Act.

Data subjects must be notified of data breaches that impact them within 48 hours of the Commission being alerted, and section 17(4) underlines the text of such communication. Sections 18-25 of the Bill

27 Section 2(5)

28 Section 3 of the Bill and Reg 2.0 of the NDPR

29 Section 4(2) (a)-(e).

30 Section 7 and 8 (1)

31 Sections 9 and 10.

outline a data subject's rights, which include the right of access, the right regarding automated decision making, the right to correction and deletion, and the right to seek legal redress. These rights are like those in the NDPR[32], except for the right to have automated processing and the right to have data processing halted.

Processing of Sensitive Data

The Bill prohibits processing data child-related under parental or guardian control by existing laws, as well as processing based on religious or philosophical beliefs, ethnic grounds, religion, race, political opinions, health, sexual orientation, or behaviour of a data subject unless otherwise provided for in the Bill or other existing laws[33]. According to the Act's interpretation section, certain types of data come under a data subject's sensitive personal data. A data processor or controller may treat sensitive personal data (the bill defines sensitive data as personal data or anything that can be designated as personal data such as health data and biometric data[34]) if the processing is required under the Bill, the data subject consent or prior consent of the parent or guardian is received before processing, regarding of a child under parental supervision[35]. Other exceptions to the processing of sensitive data are provided in sections 26(7) and Section 27(1)(a). Sensitive data about race or ethnic origin should not be processed unless it is essential for the detection and eradication of discriminatory practices and is carried out with suitable protections for the data subject's rights and freedoms.

Spiritual or religious organisations and institutions founded on religious or philosophical principles may process personal, sensitive data if it relates to their members, employees, or other persons affiliated with the organisations, if consistent with the objectives of the institutions, and is required to achieve the aims and objectives of such institutions.

Section 29 of the Bill also allows for compensation for data subjects who incur an injury because of a violation by the data controller or processing in violation of the Bill's requirements. Evidence that the data controller or processor exercised reasonable care in all situations to comply with Bill's requirements suffices as a defence on the side of the data controller or processor.

Duties of Data Controllers and Data Processors

The Bill defines the responsibilities of data controllers and processors[36]. It also provides for a data controller's vicarious liability when processing is performed on the data controller's behalf by a data processor. However, the data controller's vicarious obligation under the Bill is subject to a legally

32 Reg. 2.13.

33 Section 26(1).

34 Section 66

35 Section 26 (7).

36 Section 30 and 32.

enforceable contract between the data controller and the processor. A data controller is required to engage only a data processor who provides adequate guarantees for implementing measures, considering the data controller's responsibilities under the Bill and ensuring the protection of the data subject's rights and fundamental freedoms. Data Controllers must designate a Data Protection Officer who will oversee compliance with the bill. This is, however, subject to the Commission's regulation.

Data Location and Security

According to the Bill, data controllers and processors must only handle personal data on devices under their control, whether physically in or outside of Nigeria[37]. Data controllers and processors must use the best technological and administrative safeguards to protect personal data against breaches, destruction, and unauthorized use, alteration, or disclosure. It also requires data controllers and processors to conduct frequent tests to examine and evaluate the efficiency of their technological and organizational measures to ensure processing security[38]. This has implications for cloud computing, especially as Micro, Small and Medium Enterprises (MSME) may not be “in control” of the devices on which data is being stored. This regurgitates the importance of cloud computing for data storage.

Administration and Enforcement

Section 36 of the Bill adds the concept of an Enforcement Notice and gives the Commission the authority to issue such notifications to data controllers or processors who have violated or are reasonably suspected of violating the proposed Act's data protection principles. The notification is given to prevent a data controller or processor from processing the personal data of the person named in the notice.

Trans-Border Flow of Personal Data

According to the bill, transborder transfers of personal data may take place only if the receiving State or international organization ensures a sufficient protection. Transborder transfer of personal data may also occur where the data subject has given explicit, specific, and free consent after being informed of the risks that may arise in the absence of safeguards; the data subject's specific interests require it; and prevailing legitimate interests, particularly public interests, are provided for by law. These requirements are identical to those in the NDPR, with the exception that the present regulation's necessity for the supervision of the Attorney General has been avoided[39]. This has

37 Section 33

38 Section 34(3)

39 Section 43(1)-(3) of the Bill & Reg. 2.11 NDPR.

implications for cloud computing and supports the argument for adherence to common principles, otherwise increasing the compliance burdens on MSEs and limiting trade.

Offences and Penalties

The Bill makes illegal the unlawful acquisition, disclosure, and retention of personal data, as well as the sale of personal data and carelessness in data protection. It stipulates a punishment of 5 million nairas and/or a year in prison for unauthorized acquisition, disclosure, and keeping of personal data. It stipulates a fine of 1 million nairas per record or/and imprisonment for 5 years consecutively for the illicit selling of personal data. In the instance of illegal advertising of personal data, a fine of N500,000 naira per record and/or imprisonment for 5 years is imposed simultaneously.

It also criminalizes cases when the breach is caused by the data controller's or processor's carelessness by imposing a fine of 10 million nairas for each year of default and/or imprisonment for not less than one year. Besides imposing punishments, the court may compel the guilty individual to lose any assets, money, or equipment used or intended to be used in committing the offence to the Federal Government. The Bill also includes a provision for a Court of Law to issue orders for compensation to victims of crimes committed by convicted individuals, which is not included in the NDPR.

Records Obtained from Data Subject's Rights of Access

The Bill prohibits anybody who offers products, facilities, or services to the public from using a request for information as a condition for providing goods and services. This clause, however, does not apply when the imposition of such requirement is important for the identification of individuals or is permitted by legislation, lawful business transaction, or in the public interest.

Miscellaneous

The Bill gives the Commission the authority to evaluate, alter, or abolish regulations or rules, and it gives the Federal High Court jurisdiction over disputes about the Bill. It also allows the Commission to enter and search buildings or individuals, as well as take the property, on an ex-parte application to a Judge in Chambers if it has grounds to think that an offence under the Bill is being committed or is about to be committed.

Table 2 highlights key differences between the NDPR and data protection bill.

Table 2: NDPR vs. data protection bill (Source: Authors' illustration)

	NDPR	Data Protection Bill (2020)
Definition	The NDPR has a concise definition section that defines all the major terms in the Regulation to avoid ambiguity of any sort in the Regulation's interpretation.	The Bill's interpretation of section is lacking as it does not provide for interpreting essential terms within the bill and this leaves room for ambiguity.
Regulation	The NDPR has detailed provisions for regulating data within its implementation framework.	The bill provides that the commission will make the functions of the Data Protection Officer and Data Protection Compliance Organisation for regulating data.
Trans-Border flow of data	The transfer of data across borders requires the supervision of the Attorney General of the Federation.	The bill does not require the supervision of the Attorney General in any instance and this will reduce the bureaucracy faced by data controllers and processors in transferring data outside Nigeria
Data Storage	The Regulation	The bill does not recognize cloud data storage, and states that data processing shall only exist on devices within Nigeria's territorial jurisdiction.
Whistle Blowing	The NDPR includes provisions for whistleblowing.	The Data Protection Bill, unfortunately, lacks this feature and the non-inclusion of this may discourage data subjects from reporting breaches, allowing data controllers to leverage on this lacuna.

Shortcomings and Recommendations

The right to privacy is one of the major concerns in the newly emerging technological world and this bill could not have come at a better time, proposing ways to address vital issues such as possible harmful abuse by data controllers and processors.

To ensure the Bill actualises its full objectives, improvements will be required. The following are recommendations:

1. Sale of personal data: the bill only prohibits the sale where a person receives or discloses personal data to a third party intentionally or recklessly without the consent of the data controller, or after acquiring personal data, keeps it without the consent of the data controller. Therefore, permitting the sale of personal data monitoring such sales will be difficult and can cause abuse. Compared to another African country - Ghana, that prohibits the sale of personal data. This allows for a more effective system to protect data privacy.
2. Treatment of artificial legal persons: the bill seems to be limited to protecting data of natural persons, breach of data of artificial entities may prove detrimental to the persons in such organizations and even the business itself. Hence, the bill should be more inclusive.
3. Interpretations: The bill does not include certain relevant terms in the interpretation section such as trans-border. Hence, the interpretation section of the bill needs to be expanded.
4. Third-party processing contracts: Unlike the NDPR which stipulates that a written contract should be made between the third party and the data controller, this bill merely provides that When a data processor hires a third party to meet its obligations to the data controller, the data processor must impose the same data protection obligations outlined in its contract with the data controller, and the data processor is liable to the data controller for ensuring the third party's obligations are met. Therefore, the bill should be amended to include an express provision for the contract.
5. Cloud Data Protection: The bill does not recognise the need for data protection in the cloud. Everyday, people upload their personal data such as financial information and other forms of sensitive data to the cloud using software applications. While cloud solutions provide lower cost digitalization options for small businesses, protecting such data is essential. Thus, the bill should include data encryption provisions and data retention periods for cloud service providers. The service providers must understand and comply with the jurisdictional privacy requirements if they are to operate within the jurisdiction.
6. Role of Nigeria Data Protection Bureau and NITDA: Nigeria conceived the NDPR as an interim measure prior to substantive legislation[40]. Given the slow progress, the President approved

40 Olayinka Alao (2022). The Nigeria Data Protection Bureau And The Challenges Of Data Privacy Compliance In Nigeria - Privacy - Nigeria. <https://www.mondaq.com/nigeria/privacy-protection/1177500/the-nigeria-data-protection-bureau-and-the-challenges-of-data-privacy-compliance-in-nigeria> accessed 2 April

the establishment of The Nigeria Data Protection Bureau (NDPB) as the regulatory agency with the primary mandate of data protection and privacy in Nigeria. Without an enabling law, the full extent and scope of this body's power and duties are currently unclear, but it is reported that it merges the gains of the NDPR and will support the development of legislation for data protection and privacy[41]. It is imperative to note that there is no enabling law that establishes the Bureau, and the Bureau might have conflicting terms of scope and functions as NITDA, the Information Technology regulator, among its functions[42].However, there can be a synergy between these regulatory agencies, mirroring the approach adopted with the Nigerian Code of Corporate Governance, 2018 and the Federal Competition and Consumer Protection Act, 2018. In such a case, sector-specific regulators commit to enforcing the relevant standards in their sectors but are required to leave certain core technical issues to the technical regulator[43].

Data Protection in Other Jurisdictions

The rise of many digitally enabled markets globally means that more consumers are asked to give access to their personal data, including financial, demographic and geolocation facts. Many countries have adopted rules governing the protection of personal data and recognizing peoples' right to privacy (often in their constitutions).

One noteworthy development affecting data protection laws in the wake of the GDPR is the offshoot of several laws in many jurisdictions that closely align with the GDPR standard. Notably, African countries have updated and attempted to update extant protection/privacy laws following the GDPR. For instance, Nigeria in early 2019 repealed her extant 2013 framework for protecting personal data ("Data Protection Guidelines") and replaced it with Data Protection Regulation of 2019. Ditto for Mauritius, in 2019 that updated her protection regulation with the Laws of 2019-014 relating to the Protection of Personal Data. In 2017, Benin Republic replaced her existing 2009 data protection law with the GDPR-influenced data protection regulation. All these new regulations enshrine several commendable components of the GDPR, the rights of data subjects and the legal obligations of controllers and processors. Taking a cue from advanced jurisdictions vis-à-vis Nigeria to identify areas of likely focus and possible procedural legislations. Figure 4 presents a pictorial representation of data regulations around the world based on the intensity of data protection regulations and enforcement. In Africa, No country has heavy regulation and enforcement. Four countries have a

41 Olumide Osundolire, Toyin Bashir and Thelma Okorie, 'The Nigeria Data Protection Bureau: Key Issues For Consideration' (Banwo & Ighodalo, 2022) <https://banwo-ighodalo.com/grey-matter/the-nigeria-data-protection-bureau-key-issues-for-consideration> accessed 2 April

42 National Information Technology Development Agency Act 2007.

43 Olumide Osundolire, Toyin Bashir and Thelma Okorie, 'The Nigeria Data Protection Bureau: Key Issues For Consideration' (Banwo & Ighodalo, 2022) <https://banwo-ighodalo.com/grey-matter/the-nigeria-data-protection-bureau-key-issues-for-consideration> accessed 2 April

robust regulation and enforcement and include Senegal, Egypt, Tunisia and Morrocco. Most of the countries including Nigeria have moderate and limited regulation and enforcement.

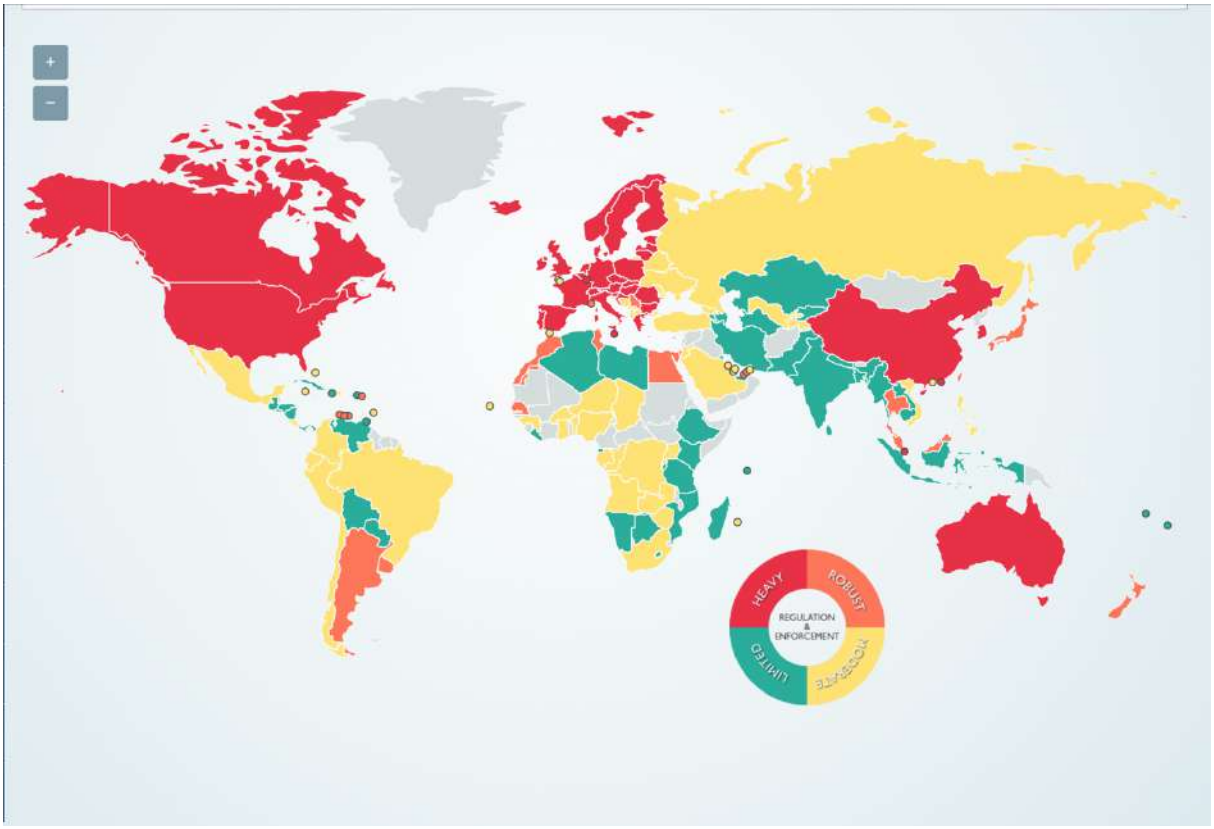

Figure 4: Data protection regulation and enforcement heatmap (Source: DLA Piper)

Based on data protection maturity, geography and privacy ranking, Table 3 summarizes data protection practices in key jurisdictions.

Table 3: Data protection across jurisdictions (Source: Authors' compilation)

	South Africa	Kenya	UK	Norway	Nigeria	Senegal
Legislation	Protection of Personal Information Act, 2013	Data Protection Act, 2019	Data Protection Act (DPA), 2018[44] is the UK's implementation of the GDPR.	The General Data Protection Regulation, 2016 & Personal Data Act, 2018.	Nigeria Data Protection Regulation, 2019	Act No 2008-12 Concerning Personal Data Protection ("**the Act"**); Decree No 2008-721 relating to the the implementation of Act No 2008-12 Concerning Personal Data Protection ("**the implementing Decree**"); Act No. 2008-08 on electronic transactions; Act no. 2016-29 amending the criminal code; Act. No. 10-2021 amending the criminal code.
Scope	Applies to any natural or juristic persons that keep records relating to personal information unless the records are subject to other legislation which protects the information more	The Act applies to personal data of subjects in Kenya documented by a data controller or processor living in or outside Kenya, either through automated or non-automated means.	Applies to everyone responsible for using personal data by strictly following the jurisdiction's 'data protection principles'	Though not a member of the EU, her GDPR rules in the establishment's context of a controller or processor of PIDs in the EU also apply to non-EU extraterritorial provisions.	Applies to all transactions that involve the processing of personal data of natural persons in Nigeria, citizens living in Nigeria or abroad.	The law governs the use of collection, storage, use, and disclosure of the personal data and information of Senegalese citizens. The data owners and data processors fall

44 In the UK, the Data Protection Act, 1998 was the initial data regulation framework designed to regulate the digital space.

	South Africa	Kenya	UK	Norway	Nigeria	Senegal
	stringently. The Act sets the minimum standard for protecting personal information.			The Personal Data Act applies to i. controllers or processors established in Norway i. ii. Processing of personal data on data subjects in Norway		within the scope of the Law. The law also covers business in ither jurisdiction if the business' means of processing is in Senegal.
Objectives	To expound on the Constitutional right to privacy and protect personal information To regulate the process of data processing. To establish an Information Regulator to enforce the Act. To create awareness of the rights and remedies to protect their personal information.	To regulate the processing of personal data and ensure that the regulation is guided by the identified principles in section 25. To protect the privacy of individuals and establish institutions to protect personal data. To make provision for the right of data subjects and provide solutions to safeguard personal data from processing not in line with the act.	The aim is to control how the Briton's PIIs should be used by organization, businesses and governments	The objective is in line with the EU GDPR (2016/679) framework relating to the processing of personal data.	To protect the right to data privacy To provide a conducive environment for transactions involving the exchange of data. Prevention of personal data manipulation To create a regulatory framework in line with best practices that facilitate competitiveness in the international space.	The Law set out to provide data protection framework, including requiring data processing notifications, setting out fundamental data subject rights, and regulating data transfers.

	South Africa	Kenya	UK	Norway	Nigeria	Senegal
Regulatory Bodies and Duties	The act establishes the Information Regulator as the regulatory body, and the powers and duties are clearly stated within the act.	The act established the Data Protection Commission to implement and enforce every provision of the act under the power of the office stipulated.	For organizations, they are expected to have a Data Protection unit headed by a DPO. In the absence of DPO, the company secretary should be addressed regarding privacy matters. Any inappropriate use of public PIIs should be reported to Information Commissioner's Office (ICO)			"Commission de Données Personnelles" ("**CDP**"). CDP is an administrative body responsible for the processing of personal information according to the provisions of the Law.
Protocols for Data Protection	POPIA is predicated on eight key principles: • Lawful collection • Limited use • Limited Processing • Information quality • Transparency • Security • Participation • Compliance with regulation	Registration of data controllers and data processors Data processors and controllers are compelled to apply to the office of the Data Protection Commission for registration. A stipulated duration of the registration certificate Publication of registered	According to the DPA 2018; Organizations must make sure the information is: ● used fairly, lawfully, and transparently ● Used for specified and explicit purpose ● accurate and, when necessary, kept up to date ● Kept no longer than necessary ● Handled in a way that ensures appropriate security, including protection against unlawful processing,	All processing of personal data must comply with all the six *GDPRs general data quality* protocol i. processed lawfully, fairly and transparently ii. Collected for specific, explicit and legitimate purposes and not processed in a manner incompatible with those purposes. Iii. adequate, relevant and not excessive iv. accurate and, when necessary, up to date	All personal data are expected to be processed following the provisions of the regulation under the governing principles of data processing. These principles include; • Lawfully processed, adequate, accurate and transparent, stored for the necessary and determined period, collected for an identified purpose, secured against breaches and cyber attacks. • Confidentiality and Accountability: The	**Notification**: Businesses must notify the CDP in respect of their processing activities except in situations stated in the Act. **Authorization**: Prior authorization is required for some types personal data such as bimetric data, data with National Indentification Number, data related to security, offences and

	South Africa	Kenya	UK	Norway	Nigeria	Senegal
		processors and controllers Periodic audit to ensure compliance. Administrative fines for failing to adhere to the provision of the act.	access, loss, destruction and/or damage.	v. kept in an identifiable form for no longer than necessary vi. kept secure.	duty of anyone entrusted with the personal data of data subjects is to care for the data.	convictions, data that include interconnection of files etc. Prior authorization is not required for some other types of data as stipulated in the act. **Notice/Opinion Regime:** The processing of personal information on behalf of the state, a public institution or local person or legal person are decided by regulatory act taken after a reasoned opinion from the CDP.
Data Localization and Data Storage	The Act prohibits the cross-border flow of personal information, except the conditions for exemption are satisfied. Cross-border transfer of data is allowed when the recipient country uphold data protection	The act includes a provision for data localization. No data about Kenyans are not transferable outside Kenya except with the consent of the data subject or proof of sufficient data protection provided to	The DPA proviso is that organizations must give a copy of data they hold to the data subject as soon as possible, and within 1 month, at most However, in certain circumstances - with complex or multiple	Makes provision for cross border transfer of data. The processing, storage and cross-border transfer of data must also satisfy at least **one condition** for the processing and localising personal data. These are;	Cross border transfer of data is subject to the provisions within the regulation and the supervision of the Honourable Attorney General of the Federation (HAGF). The regulation provides situations when data transfer across borders is allowed, to include; where	The Act prohibits transfer of data to another country unless the foreign country provides sufficient evidence of data subject's protection and privacy. The Act considers country

	South Africa	Kenya	UK	Norway	Nigeria	Senegal
	of the same standard entrenched in the Act or based on the consent of the data subject or in the situation where it is important to close a contract between the data subject and the responsible party.	the data protection commission. Personal data is stored for a defined time-limit and periodic review for the need for data storage.	requests, the organization can take a further two months to provide data where they are expected to tell the data subject: ● Within one month of request ● Why there's a delay.	• Carried out with data subject consent. • Necessary for the performance of a contract with the data subject. • Necessary for compliance with a legal obligation. • Necessary in order to protect the vital interest of the data subjects. • Necessary for the public interest in the exercise of official authority. • Necessary for the controller's or recipient's legitimate interest, except where overridden by the interests of the data subjects.	the country or international organization shows proof of adequate data protection and sound legal system, presence of functional supervisory authority in the foreign country that enforces alignment with the data protection rules, consent of data subjects. Important public interest, data needed to conclude a transaction between the data subject and controller and other situations documented in the regulation. Data is kept or stored for a specific and ideal time.	members of 'Association Francophone des Autorités de Protection des Données Personnelles' to have sufficient protection for data subject. Other countries are examined on a case by case basis following certain conditions stipulated in the Act. The act provides for countries not having sufficient protection for data subject by stating other criteria.
Key Players	**Data Subjects:** The owner of the information **The Responsible Party:** The person who determines how and why to process **The Operator:** the person who processes	**Data subjects:** The person about which information is collected. **Data Commissioner:** head of the Data Protection Commission	**Data Subject**: An individual that is the subject of the relevant personal data **Authorities Responsible**: The ICO oversees the UK GDPR.	**Data Subject:** The owner of the information or the individual who is the subject of the personal data. **Data Controller or Processor:** The GDPR provides for a controller	**Data Subject:** A person who is the subject of the personal data **Data Processor:** Any entity, which alone or jointly processes personal data on behalf of the data controller. **Data Controller:** Person (s) that determines how	**Data Controllers:** Data controllers are subject obligations that include transparency, security and confidentiality.

	South Africa	Kenya	UK	Norway	Nigeria	Senegal
	personal information on behalf of the responsible party.	**Data controllers and Processors:** Person(s) that determine the purpose, means of processing and engage in the actual processing of personal data.	DPOs handle data organizational privacy.	or processor-based in and outside of the EU to include anybody who (1) offers goods and services to individuals in the EU; (ii) monitors individuals within the EU	personal data should be processed.	**Data Protection Officer:** Businesses are expected to have a data protection officer appointed by data controller. **Data Focal Point**: Every ministries is expected to have a data focal point for the purpose of declaration of files in the database and census of files related to personal data. **Data Subject:** The owner of the information has specific right to information from the data controller as stipulated in the Act. CDP: The CDP is the regulator. It trains data protection officers, inform data subjects and controllers of their rights and obligations, in charge

	South Africa	Kenya	UK	Norway	Nigeria	Senegal
						of the legislation and regulatory framework for data processing and perform other duties has documented in the Act.
Existence of definition	Concise and related to personal data.	Concise and related to personal data.	As defined under the EU GDPR framework.		Concise definition of data and personal data.	Concise definition of personal data as stated in Article 4 of the Act.
Regulatory & Enforcement Level	Moderate	Limited	Heavy	Heavy	Moderate	Robust
Privacy Ranking[45]	27	57	12	1	79	54

45 The internet privacy ranking ranks countries based on the internet privacy score or index. Internet privacy is measured based on data collected on press freedom, data privacy laws, democracy statistics, freedom of opinion and expressions and cybercrime legislations. Available at Internet Privacy Index – 2022 - BestVPN.org

Conclusion

Regardless of the looseness in the protection and privacy of personal data in Nigeria, the emergence of digital technology in the business environment raises the risk of violating the fundamental human rights if nothing is done to protect this personal information. Hence, as we develop in an ever-changing digital space, adequate data protection and privacy practices that align with best practices are foundational to Nigeria and her citizens. It is the responsibility of the government to protect the people by ensuring openness and optimising the benefits of the digital economy, without restricting choices. Lack of sufficient data protection and privacy reduces business confidence and consumer trust. Too much data protection impedes innovation, the productivity and growth of micro, small and medium enterprises (MSMEs), while also increasing compliance burdens. Thus, we need laws that set a conducive environment to promote businesses and international competitiveness, provide clarity regarding the fundamental right to privacy, and safeguard the nation's sovereignty.

The diverse interest by individuals, government and businesses present frictions on the focus of data protection and privacy legislation and processes. Individuals are mostly interested in their right to privacy and the ability to engage in online transactions safely; businesses agitate about how to meet the regulatory standards without stifling innovations and trade; while the government is concerned about threats to the security of the nation and sovereignty. Adopting the identified core data protection principles closes domestic implementation gaps and makes the economy internationally competitive and a destination for trade and investment. In ensuring international competitiveness, trade, and innovation, policy clarity about the cross-border data transfer and data localization are crucial, taking the pros and cons into cognizance. The legislation should level the playing field with the understanding of in-country digital infrastructure and resources, and accommodating to all entities, regardless of size. For example, a small business owner may not find local cloud storage services affordable, because of higher costs (economies of scale/unit economics) or may not have access to a local node for the services required. The burden of paying for cloud services in foreign currencies is yet another challenge, as Nigeria seeks to manage her foreign reserves. The dearth of scale local technology providers and affordable and accessible hosting facilities limit availability. These are foundational to building a digital economy. In addition, the bill should be mindful of the compliance burden, especially for MSMEs taking part in international or regional trade, but that lack of access to resources to maintain compliance.

To address these challenges and level the playing field, the provisions of data localization should be based on data sensitivity and risks. The data classification in Table 4 illustrates the data by type and risk and sensitivity classification is one such model. Such a data classification framework ensures the proper processing of sensitive data, reducing the risk of data privacy and protection.

Table 4: Data classification (Source: Authors' illustration)

DATA TYPE	DESCRIPTION	SENSITIVITY	RISK
RESTRICTED	Highly sensitive data that can increase political, legal and financial risks	High	High
CONFIDENTIAL	Sensitive data that can have negative effects if compromised	Moderately high	Medium
INTERNAL	Internal data, not for public consumption	Low	Low
PUBLIC	Data that is freely available to the public	Low	Low

Restricted data is highly sensitive data and can lead to political, legal, and financial risks. Confidential data is sensitive data that can have a negative effect when compromised. These kinds also require a high level of control and protection. Internal data is for internal use within an organisation or institution; while the public is freely available and requires no data protection.

Nigeria's economy is in transition and requires policies and regulations that will enable a conducive and enabling environment. The benefits of data protection are significant to Nigeria's economy as we seek to diversify and build a digital economy. Thus, a national, holistic and coordinated approach led by a single central regulator, working alongside other government ministries, departments and agencies (MDAs) is fundamental and reducing the administrative burden of sector-specific regulators.

Acknowledgements

This work would not have been possible without the support of the American Business Council.

Authors

Olayinka David-West, Zeena Mustafa, Hammed Akanji and Adewunmi Otonne of the Lagos Business School authored this white paper.

About Lagos Business School

Lagos Business School (LBS) is the graduate business school of Pan-Atlantic University (formerly Pan-African University). LBS offers academic programmes, executive programmes and short courses (customised to specific company needs, and open-enrolment courses) in management education. LBS is ranked among the best in Africa as it systematically strives to improve the practice of management on the continent.