

# POLICY BRIEF 2024



## Strengthening Data Protection: Ensuring Privacy and Security for Nigerian Citizens

Policy Brief

# **Strengthening DataProtection: Ensuring Privacy and Security for Nigerian Citizens**

By

**Jake Okechukwu Effoduh**  
(Assistant Professor, Lincoln Alexander School of Law)

And

**Odeh Friday Odeh**  
(Country Director, Accountability Lab Nigeria)

**January 2024**

Design by:  
**Ifeyolu N. Hyacinth**, Stears Consul LTD.

This Policy Brief examines the existing data protection regime both in Nigeria and globally and suggests ways to improve the data protection efforts in Nigeria. It considers Nigeria's principal data protection laws, generally applicable across all sectors (including public and private institutions). By examining and juxtaposing some of the exemptions in legislation, an opportunity for abuse of data subjects' rights may have been inadvertently created by laws that were enacted to do otherwise. This Policy Brief proffers preferable outcomes that may guide engagement with policymakers to rectify this situation.



## Strengthening Data Protection: Ensuring Privacy and Security for Nigerian Citizens

I

## International Regimes on Data Protection

II

## Data Protection Laws in Nigeria

III

## Data Protection Failures

IV

## Strengthening Nigeria's Data Protection Framework

V



## **Strengthening Data Protection: Ensuring Privacy and Security for Nigerian Citizens**

# Background

The United Nations has revealed that 137 out of 194 countries have some form of data protection regime, a global coverage unlike ever before.<sup>1</sup> A breakdown of the report reveals that in total, 71 percent of countries have privacy regulations, 9 percent of countries have draft legislation, and 15 percent of countries have no legislation.<sup>2</sup> In addition, another report by Gartner, a provider of research and consulting services for businesses in the IT sector, reveals that by 2024, modern privacy regulation will cover the majority of consumer data.<sup>3</sup> The latter inspires confidence but is unsurprising and perhaps even overdue, considering the global pace of the digitalization of information and the globalization of data privacy concerns.<sup>4</sup>

There have been pockets of efforts to introduce data protection principles into Nigerian legislation.<sup>5</sup> However, the first data protection-focused legislation was the Nigeria Data Protection Regulations (“NDPR”) 2019. This was the forerunner to the 2023 Nigerian Data Protection Act (the “NDPA” or the “Act”), signed into law in June 2023. The NDPA represents a significant milestone in Nigeria’s journey to ensuring responsible data processing, promoting transparency, and fostering a culture of data protection.<sup>6</sup> However, despite these legislative efforts, data privacy breaches and other data privacy issues remain abundant.

The right to data protection may be seen as a recent entry into the slew of human rights protections because several international statutes and covenants do not strictly have data privacy provisions. However, some existing provisions of international treaties accommodate data privacy obligations. For instance, both Article 12 of the Universal

---

1 The United Nations Conference on Trade and Development, ‘Data Protection and Privacy Legislation Worldwide’ Accessible here: <https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>

2 Ibid.

3 Gartner, ‘Gartner Reveals Top Eight Cybersecurity Predictions for 2023 – 2024’ (28 March 2023) Accessible here: <https://www.gartner.com/en/newsroom/press-releases/2023-03-28-gartner-unveils-top-8-cybersecurity-predictions-for-2023-2024>. The same report reveals that less than 10 percent of organizations will have successfully weaponized privacy as a competitive advantage in 2024. This lends credence to the fact that privacy laws act as business enablers and not destroyers, contrary to what is the position in some quarters.

4 Case in point being the Snowden Scandal that broke in 2013. It was a huge reveal by a former United States National Security Agency (NSA), Edward Snowden, to the effect that the NSA was collecting the phone records of tens of millions of Americans, having tapped directly into the servers of nine internet firms: including Facebook, Google, Microsoft, and Yahoo in a surveillance programme that was code-named ‘Prism’. The scandal spurred conversations regarding data privacy and espionage globally. (‘Edward Snowden: Leaks that Exposed US Spy Programme’ (17 January 2014) Accessible here: <https://www.bbc.com/news/world-us-canada-23123964>)

5 There are pockets of Nigerian laws that have data protection provisions such as the Freedom of Information Act, Cybercrimes Act, the Consumer Code of Practice Regulations 2007, the National Identity Management Commission Act.

6 O. M. Ayotebi (SAN), ‘An Assessment of the Effect of the Nigerian Data Protection Act (NDPA), 2023 on Data Privacy in Nigeria’ Accessible here: <https://omaplex.com.ng/an-assessment-of-the-effect-of-the-nigerian-data-protection-act-ndpa-2023-on-data-privacy-in-nigeria/>



## International Regimes on Data Protection



Declaration of Human Rights of 1948,<sup>7</sup> and Article 17 of the International Covenant on Civil and Political Rights of 1966 (the “ICCPR”) <sup>8</sup> provide that no one shall be subjected to arbitrary or unlawful interference with their privacy, family, home, or correspondence; or unlawful attacks on their honour and reputation. Ordinarily, by protecting privacy, this provision can include a prohibition against all forms of interference, including those concerning personal data.

However, there have been deliberate efforts to integrate data privacy requirements into international statutes. For example, in the extension of the right to privacy enshrined in the ICCPR, the United Nations General Comment No. 16 provides specific rules on data protection. Some of its provisions include that the collection and storage of personal information on computers, in databases or other devices, whether by public or private bodies, must be regulated by law<sup>9</sup>. Furthermore, states are mandated to take adequate measures to ensure that information concerning a person’s private life does not reach the hands of persons not authorized by law to receive, process, and use it. Individuals also have the right to determine what information is being held about them and for what purposes and to request rectification or elimination of incorrect information, etc. <sup>10</sup>

The specific United Nations instrument dealing with data protection is the 1990 General Assembly Guidelines for the Regulation of Computerized Personal Data Files (“Computerized Personal Data Files Guidelines”). <sup>11</sup> The Computerized Personal Data Files Guidelines provide the procedures for implementing regulations concerning computerized personal data files by various states. Other relevant provisions include the requirements that information about persons should not be collected or processed in an unfair or unlawful manner,<sup>12</sup> and that computerized personal data files be protected against human dangers such as unauthorized access and fraudulent misuse of data or contamination by computer viruses;<sup>13</sup> and requirements that the purpose of data collation should be both legitimate and specified. <sup>14</sup> Unfortunately, the Computerized Personal Data Files Guidelines are not binding and serve only a directive function.

Another non-binding international statute with data protection provisions is the 1980 Organisation for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (the “OECD Guidelines”). The OECD Guidelines are touted as the first international instrument to lay out specific conditions and criteria for safeguarding citizens’ private information.<sup>15</sup> It served as a

7 Adopted by the United Nations General Assembly in Paris on 10 December 1948, the UDHR was a direct response to the “barbaric acts” which characterized the Second World War. The document contains 30 articles that speak to the rights and freedoms that belong to all of humanity regardless of sex, colour, creed, religion, or other characteristics. (Culled from the Amnesty International page here: <https://www.amnesty.org/en/what-we-do/universal-declaration-of-human-rights/>).

8 The ICCPR is a multilateral treaty that was adopted by the United Nations General Assembly Resolution 2200A(XXI) in 1966 after the 35th state ratified it. Its purview is over civil and political rights, and has provisions that touch on the right to life, freedom of assembly, electoral rights, and fair trial, etc.

9 See General Comment No. 16, the International Covenant on Civil and Political Rights (the “ICCPR”).

10 Ibid.

11 This was adopted by the United Nations General Assembly Resolution 45/95 of December 14, 1990.

12 Principle 1.

13 Principle 7.

14 Principle 3.

15 The 1980 Organisation for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data can be found here: <https://bj.a.ojp.gov/sites/g/files/xyckuh186/files/media/>

forerunner to another binding international instrument on data protection, the Convention for the Protection of Individuals concerning Automatic Processing of Personal Data (the “Convention 108”).<sup>16</sup> The Convention 108’s purview is on all data processing carried out by individuals in both the private and public sectors, with its reach even extending to the judiciary and law enforcement authorities. It makes copious provisions for the rights of data subjects,<sup>17</sup> provides for transborder flows of personal data, data security,<sup>18</sup> transparency of processing, etc.<sup>19</sup>

In the African context, the African Charter on Human and Peoples’ Rights (the “African Charter”) does not contain an express provision on the right to privacy. However, it has been argued that the right can – and should – be read into the African Charter through to the right to respect for life and integrity of the person,<sup>20</sup> the right to dignity<sup>21</sup>, and the right to liberty and security.<sup>22</sup> However, several regional African laws have direct bearings on data privacy/protection.

Remarkably, on June 27, 2014, the African Union adopted the African Union’s Convention on Cyber Security and Personal Data Protection (the “Malabo Convention”).<sup>23</sup> The Malabo Convention is a framework convention meant to provide general rules and principles on three broad themes: personal data protection, electronic commerce, and cybersecurity and cybercrime on the continent.<sup>24</sup>

In the West Africa sub-region, the Economic Community of West African States (ECOWAS)’s<sup>25</sup> Supplementary Act on Personal Data Protection within ECOWAS (the “ECOWAS Supplementary Act”) makes provisions for data protection for member states, specifically obligating member states to establish a legal framework for the protection of data privacy. The ECOWAS Supplementary Act also establishes principles guiding the processing of personal data,<sup>26</sup> sets out the rights of data subjects,<sup>27</sup> as well as obligations of personal data controllers,<sup>28</sup> amongst others.

---

document/oecd\_fips.pdf

16 Convention 108 is a Council of Europe treaty that opened for signatures on 28 January 1981. It has been acceded to by all the members of the Council of Europe, as well as non-Council of Europe members. Parties stand at 55 as of the time of writing this policy brief.

17 Article 9 of Convention 108.

18 Article 14 of Convention 108.

19 Article 8 of Convention 108.

20 Article 4 of the African Charter.

21 Article 5 of the African Charter.

22 Media Defence, ‘Media and Security Online’. Accessible here: <https://www.mediadefence.org/ereader/publications/advanced-modules-on-digital-rights-and-freedom-of-expression-online/module-4-privacy-and-security-online/scope-and-the-right-to-privacy/>

23 However, the Malabo Convention did not come into force till June 8, 2023, 30 days after the fifteenth. instrument of ratification of the convention was deposited at the AU headquarters by Mauritania.

24 Yohannes Eneyew Yalew, ‘The African Union’s Malabo Convention on Cyber Security and Personal Data Protection enters into force nearly after a decade. What does it mean for Data Privacy in Africa or beyond?’ (15 June 2023) Accessible here: <https://www.ejiltalk.org/the-african-unions-malabo-convention-on-cyber-security-and-personal-data-protection-enters-into-force-nearly-after-a-decade-what-does-it-mean-for-data-privacy-in-africa-or-beyond/>.

25 ECOWAS is a regional political and economic union of all fifteen countries that make up the West African subcontinent.

26 Article 23 of the ECOWAS Supplementary Act.

27 Articles 38, 39, 40, and 41 of the ECOWAS Supplementary Act.

28 Articles 42 to 45 of the ECOWAS Supplementary Act.





## Data Protection Laws in Nigeria

# Findings

## A

### The Nigerian Data Protection Act ('NDPA, the Act') 2023

The scope and enforceability of the NDPA are limited by section 3(2)(a–c) of the Act, which generally provides that subject to the rights and freedoms under the Constitution and its limitations, the obligations under Part V of the Act, asides sections 24 (principles of personal data processing), 25 (lawful basis of personal data processing), 32 (appointing data protection officers), and 40, will not apply to a data controller or processor, where a competent authority carries out personal data processing concerning criminal offences, national public health emergency, or national security.

The effect of this exemption is that purposes covered by subsections (a–c) above are not required to obtain consent validly, provide information about the processing to the data subject, conduct data privacy assessments, are not bound by the regular obligations on data controllers and processors, sensitive personal data principles, or consent concerning children or persons lacking the capacity to consent.

This wide range of exemptions has allowed for the acquisition of advanced surveillance technologies with minimal regard for safeguards around real-world deployment. Over the years, Nigerian law enforcement agencies have exploited the exemptions granted them to acquire tools for social me-

***This wide range of exemptions has allowed for the acquisition of advanced surveillance technologies with minimal regard for safeguards around real-world deployment.***

dia mining, spyware, and communication interception. In the absence of requirements like conducting data privacy impact assessments, it is difficult to assess the proportionality or necessity of these tools in the harms that law enforcement agencies seek to curb or prevent.

## B

### The Nigerian Data Protection Regulation (NDPR) 2019

Article 4.1 of the NDPR requires all public and private organizations that control the data of natural persons to make their respective data protection policies available to the public, which shall conform to the NDPR. The NDPR was issued on 25 January 2019, and this provision was to be implemented within three months of its issuance.

A review of the websites of the Office of National Security Adviser, Department of State Services, Ministry of Defense, or the Nigeria Police Force does not indicate the presence of a Privacy Policy, which would usually indicate the data protection and management measures of a data controller or processor. The NDPR Implementation Framework

## C

## The NDPR Implementation Framework

clarifies in Article 2.1 that the NDPR will not apply to using personal data for national security, public health, safety, and order. It will also not apply to the investigation of criminal and tax offences. This, in effect, provides a further exemption for law enforcement agencies from having to provide their data protection policies to the public.

## D

## The Guidelines for the Management of Personal Data by Public Institutions ('the Guidelines') 2020

Ordinarily, the provisions of the Guidelines ought to cover all or most of the exemptions in the previous laws. Article 2.1 provides that public institutions are obligated to protect personal data where it is processed and that all forms of personal data shall be protected in the NDPR and other laws or regulations in force in Nigeria. Article 2.4 further provides that a higher standard of consent-seeking will be applicable when processing sensitive personal data.

Article 2.5, however, waters this down by exempting this higher standard where the processing involves health emergency, national security, and crime prevention. Sensitive personal data under the Act includes genetic and biometric data, race, or ethnic origin, religious or similar beliefs, health status, sex life, political opinions or affiliations, and trade union memberships. Section 30(1) of the Act provides insights on how sensitive personal data should be treated, requiring, for instance, that sensitive personal data shall not be processed except where consent is obtained, necessary for purposes relating to employment or social security, protecting vital interests, the conduct of legal proceedings, or the substantial public interest, proportionate to the aim pursued, and the provision of measures to safeguard the fundamental rights, freedoms, and interests of the data subject.

As such, law enforcement agencies, by a combined reading of the Act and Guidelines, are largely free to collect and process data about sexuality, religious beliefs, and political affiliations, whether it is relevant to the investigation in question, with minimal accountability measures in place.

The fulcrum on which the gamut of data protection laws in Nigeria rests is the constitutional provision granting citizens the right to privacy. Section 37 of the Constitution of the Federal Republic of Nigeria 1999 (as amended) (the "Constitution") provides that "the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected."

Aside from the Constitution, other legislation also touches on data protection in Nigeria. One such is the Freedom of Information Act 2011 (the "FOI Act").<sup>29</sup> Section 14 (1) of the FOI Act empowers a public institution to deny a request for information that contains personal data.

<sup>29</sup> The FOI Act was enacted on May 28, 2011, to, amongst others, make public records and information more freely available, provide public access to public records and information and protect serving public officers from the adverse consequences for disclosing certain kinds of official information without authorization.

Section 14 (1) of the FOI Act empowers a public institution to deny a request for information that contains personal data. The FOI Act defines personal information as any official information held about an identifiable person but does not include information that bears on the public duties of public employees and officials.<sup>30</sup> The FOI Act also exempts privileged communications from the category of information that public institutions can divulge.<sup>31</sup> This provision laid the foundation for the judicial pronouncement that extended the requirement for privileged communication to specific categories of persons, e.g., banks, to maintain the confidentiality of their clients even where such a requirement is not strictly on account of the law.<sup>32</sup>

Additionally, the Cybercrimes (Prohibitions, Prevention, etc.) Act 2015 makes it an offence for any person to intercept, by technical means, non-public transmissions of computer data, content, or traffic data.<sup>33</sup>

The Nigerian Communications Commission-issued Consumer Code of Practice Regulations 2007 mandates licensees to ensure that the collection and maintenance of information on individual consumers is protected against improper or accidental disclosure.<sup>34</sup>

The Central Bank of Nigeria Consumer Protection Framework (the “CBN Protection Framework”)<sup>35</sup> provides that financial institutions shall take appropriate measures to ensure that consumers’ financial and personal information is always protected and shall not be released to a third party without the consent of the consumer, except as required by law.<sup>36</sup>

Similarly, the National Identity Management Commission (NIMC) Act 2007<sup>37</sup> provides that no person or body shall have access to the data or information contained in its database with respect to a registered individual concerned, except with the consent of the person or the authorization of the NIMC.<sup>38</sup>

Additionally, the Credit Reporting Act of 2017 makes it mandatory that the credit information of individuals be kept confidentially and should only be shared with the consent of the individual concerned.<sup>39</sup>

For a long time, these peripheral legislations regulated data protection in Nigeria until 2019 when

---

30 Section 30(3) of the FOI Act.

31 Section 16 of the FOI Act.

32 *Habib Nigeria Bank Limited v Fathudeen Syed M. Koya* [1992] 7 NWLR Pt. 251.

33 Section 12 of the Cybercrimes Act.

34 Section 35 (1) of the NCC Consumer Code of Practice Regulations 2007.

35 The CBN Consumer Protection Framework issued by the apex bank in Nigeria is to guide the effective regulation of consumer protection practices of Financial Institutions (FIs) under the regulatory purview of the CBN to ensure that consumers of financial services are adequately protected and treated fairly. It documents the roles and responsibilities of the CBN, the FIs and the consumers in ensuring that the standards set, are met.

36 The CBN Consumer Protection Framework 2016.

37 The NIMC Act establishes the NIMC as the statutory body in charge of Nigeria’s identity management systems. The NIMC oversees the capturing of the personal data of Nigerians for the purpose of issuance of an identity card number.

38 Section 26 of the NIMC Act.

39 Section 9 of the Credit Reporting Act.

the National Information Development Technology Agency (NITDA)<sup>40</sup> released the NDPR.<sup>41</sup>

As communicated above, this was followed by the Nigeria Data Protection Regulations Implementation Framework 2020, which explained and extended the provisions of the NDPR.<sup>42</sup> However, the primary legislation that governs data protection in Nigeria is the Nigeria Data Protection Act (NDPA) 2023.<sup>43</sup>

The NDPA sets up a regulatory framework for the regulation of data privacy in Nigeria, with primary implementation functions<sup>44</sup> foisted on the Nigerian Data Protection Commission (the “NDPC” or the “Commission”).<sup>45</sup> The Act has both local and extraterritorial reach and is generally applicable to the processing<sup>46</sup> of personal data<sup>47</sup> by data subjects, whether by automated means or not.<sup>48</sup> The NDPA specifically applies where a data controller<sup>49</sup> or data processor<sup>50</sup> is domiciled in, resident in, or operating in Nigeria,<sup>51</sup> where the processing of personal data occurs in Nigeria<sup>52</sup> or the data controller or data processor is not domiciled in, resident in, or operating in Nigeria but is processing personal data of a data subject in Nigeria.

40 NITDA is the statutory agency with the responsibility for planning, developing, and promoting the use of information technology in Nigeria.

41 The NDPR was a “placeholder,” so to speak, as it was a subsidiary legislation and could not exceed the powers granted by law to its enabling statute. There were queries regarding the scope of its applicability and whether it imposed binding obligations on Nigerians. However, in the interim, that is, before the enactment of the NDPA, the NDPR carried out the following functions: safeguarding the rights of natural persons to data privacy; fostering safe conduct for transactions involving the exchange of Personal Data; preventing manipulation of Personal Data; and ensuring that Nigerian businesses remain competitive in international trade, amongst others.

42 It is important to note that the NDPA does not invalidate the NDPR. In fact, the Act is express that the NDPR will continue to serve complementary roles to the NDPA until the former is expressly repealed or a new regulation pursuant to the NDPA is enacted.

43 The Act was signed into law on 12 June 2023 by President Bola Ahmed Tinubu.

44 The Commission has several functions, including to: (i) promote awareness of data controllers and data processors of their obligations under the Act; (ii) ensure the deployment of technological and organisational measures to enhance personal data protection; (iii) foster the development of personal data protection technologies in accordance with recognized international good practices and applicable international law; (iv) participate in international fora and engage with other national and regional authorities responsible for data protection with a view to developing consistent and efficient approaches to regulation of cross-border transfers of personal data; (v) advise the government on policy issues relating to data protection and privacy; (vi) collect and publish information with respect to personal data protection, including personal data breaches; and (vii) receive complaints relating to violations of the NDPA or regulations issued pursuant to the NDPA, etc. (Section 5 of the NDPA).

45 Section 4 of the NDPA.

46 “Processing” as used in the NDPA, means any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, and does not include the mere transit of data originating outside Nigeria.

47 Under the NDPA, “Personal Data” refers to any information relating to an individual, who can be identified or is identifiable, directly, or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, psychological, cultural, social or economic identity of that individual.

48 Section 2(1) of the NDPA.

49 The NDPA defines “Data Controller” as an individual, private entity, public Commission or agency, or any other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

50 Under the NDPA, a “Data Processor” is referred to as an individual, private entity, public authority, or any other body who or which processes personal data on behalf of or at the direction of a data controller or another data processor.

51 Section 2(2)(a) of the NDPA.

52 Section 2(2)(b) of the NDPA.



The NDPA establishes a stringent set of rules<sup>53</sup>, which data controllers and data processors have to abide by while processing the data of citizens. Of note are the extensive rights data subjects enjoy under the new regime.<sup>54</sup> Where any of these rights are infringed upon, the data subject has the right to seek redress under the law. The Act provides that a data subject who is aggrieved by the action of a data controller or processor has the right to lodge a complaint with the Commission.<sup>55</sup> Where a data subject is unsatisfied with any order given by the Commission, such a data subject is at liberty to the Court for judicial review within 30 days after the order was made.

However, the NDPA also provides for instances where the principles laid down in the act would not apply to data processing in Nigeria, providing respite for certain categories of people to violate established data processing requirements, albeit lawfully.<sup>56</sup>

---

53 These set of rules are known as grounds for “lawful processing”. Under the NDPA, grounds for lawful processing of personal data include the following: (a) where the data subject has given and not withdrawn consent for the specific purpose or purposes for which Personal Data is to be processed; (b) where processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract; (c) where processing is necessary for compliance with a legal obligation to which the Data Controller or Data Processor is subject; (d) where processing is necessary in order to protect the vital interests of the Data Subject or of another natural person; where processing is necessary for the performance of a task carried out in the public interest or in exercise of official public mandate vested in the Data Controller; or (e) where processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or Data Processor, or by a third party to whom the data is disclosed. (Section 25 of the NDPA).

54 Under the NDPA, the rights of data subjects include the following: (1) Right to information: Data subject have the right to obtain information from data controllers regarding the processing of their personal data. (2) Right to data portability: this is the right of data subjects to receive a copy of their personal data in a commonly used electronic format. (3) Right to withdrawal of Consent: Data subjects are empowered to withdraw their consent to the processing of personal data at any time. (4) The right to object to automated decision making: Data subjects have the right to not be subject to decisions based solely on automated processing of personal data. (5) The right to data portability (See sections 34 – 37 of the NDPA generally).

55 Section 46 of the NDPA.


56 The NDPA does not apply to processing carried out by individuals for purely personal, recreational or household purposes. (Section 3 (1) of the NDPA). It does not apply to a data controller or data processor when processing of personal data is: a). carried out by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; b). carried out by competent authorities for the purposes of prevention or control of a national public health emergency; c). carried out by competent authorities as necessary for national security; d). in respect of publication in the public interest for journalism, educational, artistic, and literary purposes to the extent that such obligations and rights would be incompatible with such purposes; or e). necessary for the establishment, exercise, or defense of legal claims, whether in court proceedings, or in an administrative or out-of-court procedure. (Section 3 (2) of the NDPA). The Nigeria Data Protection Commission (the “Commission”) may also, by regulation, exempt certain types of personal data or processing from the application of the Act.



## Data Protection Failures


It could be argued that Nigeria has a robust data protection framework. However, some data privacy issues persist. Some of them are as follows:

### 1. Legal Interference with Private Data:



Nigeria's data protection regime exists alongside numerous legal provisions that empower certain entities, the government, especially, to interfere with or intercept citizens' personal information legally.<sup>57</sup> The Nigerian government, especially, makes no secret of its intentions either to interfere with citizens' private data or regulate same.<sup>58</sup> These powers of interference (which are extensive in most cases), with little or no oversight powers granted to any entity, dilute the effectiveness of the existing data protection laws. This is because the laws legalizing interception often exclude the application of the relevant data protection laws.


### 2. Advancement of Technology:



This is not a unique Nigerian problem, but a challenge faced by the Nigerian data protection system. The rate of the advancement of technology poses a challenge for data protection globally. On the one hand, it is easier now than ever for data to be collated and stored, sometimes without data subjects' (conscious) acquiescence. On the other hand, the regulatory instruments providing oversight over the subject and the sector struggle to keep up as nefarious elements often find innovative ways to get around enforcement mechanisms set up by the government.

***The rate of the advancement of technology poses a challenge for data protection globally.***

### 3. Weak Enforcement Apparatus:



The brazen infringement of the data of private citizens by the government is especially a pointer to the weak enforcement systems in the country. The NDPA established the Nigerian Data Protection Commission (the "NDPC") as the body to enforce the provisions of the Act. However, its effects have hardly been felt since the inception of the NDPA.

---

<sup>57</sup> For instance, the NCC has the power to, during a public emergency or in the interest of public safety, allow authorized interception of communications (Section 147 and 148 of the NCC Act 2003.), the Cybercrimes Act also empowers a judge to order a service provider or a law enforcement agent to collect, record, permit or assist competent authorities with the collection or recording of content data and/or traffic data associated with specified communications transmitted by means of a computer system (section 39 of the Cybercrimes Act), the Lawful Interception of Communications Regulations 2019 provide the basis, process, and framework for the interception of communications and divulgence of same by certain entities in Nigeria.

<sup>58</sup> As recent as October 2023, it was revealed that there were plans underway to amend the National Broadcasting Commission (NBC) Act 2004, which sets up the NBC, to give the NBC power to regulate social media.



#### **4. Lack of Awareness:**

One key challenge with enforcing data protection laws in Nigeria is unawareness. Many people for whom the laws are made are not conscious of what amounts to data privacy infringement. Even those who may be aware when their rights are violated may downplay the risks that such invasions can cause. Additionally, many data subjects are unaware of the options open to them upon an infringement of their data privacy rights.



#### **5. Lack of Judicial Expertise and Precedents:**

There is a dearth of judicial authorities about data privacy and protection. This is in part due to the lack of enforcement of data privacy. In addition, there is the challenge of the lack of judicial expertise as the judiciary may not have enough knowledge about data protection, given that is quite a niche area.



#### **6. Balancing Rights and Obligations:**

The NDPA, and other data protection laws, place certain responsibilities on data controllers and processors.<sup>59</sup> However, some of these data controllers and processors may lack the means to live up to the expectations, even when they have the intentions to. Additionally, there could arise legitimate necessities to lawful processing, beyond what the laws currently contemplate. E.g., interception of citizens' phone logs may be necessary to safeguard the nation's security. Hence, there is a need to balance these competing interests to ensure that data protection needs are not compromised and that at the same time, players are not overly burdened with responsibilities.

---

<sup>59</sup> These obligations include the duty to carry out a data privacy impact assessment in some cases (section 28 of the NDPA), obligations that arise with relation to sensitive personal data and children's data (sections 30 & 31 of the NDPA), appointments of data protection officers by data controllers of significant importance (section 32 of the NDPA), amongst others.



## **Strengthening Nigeria's Data Protection Framework**

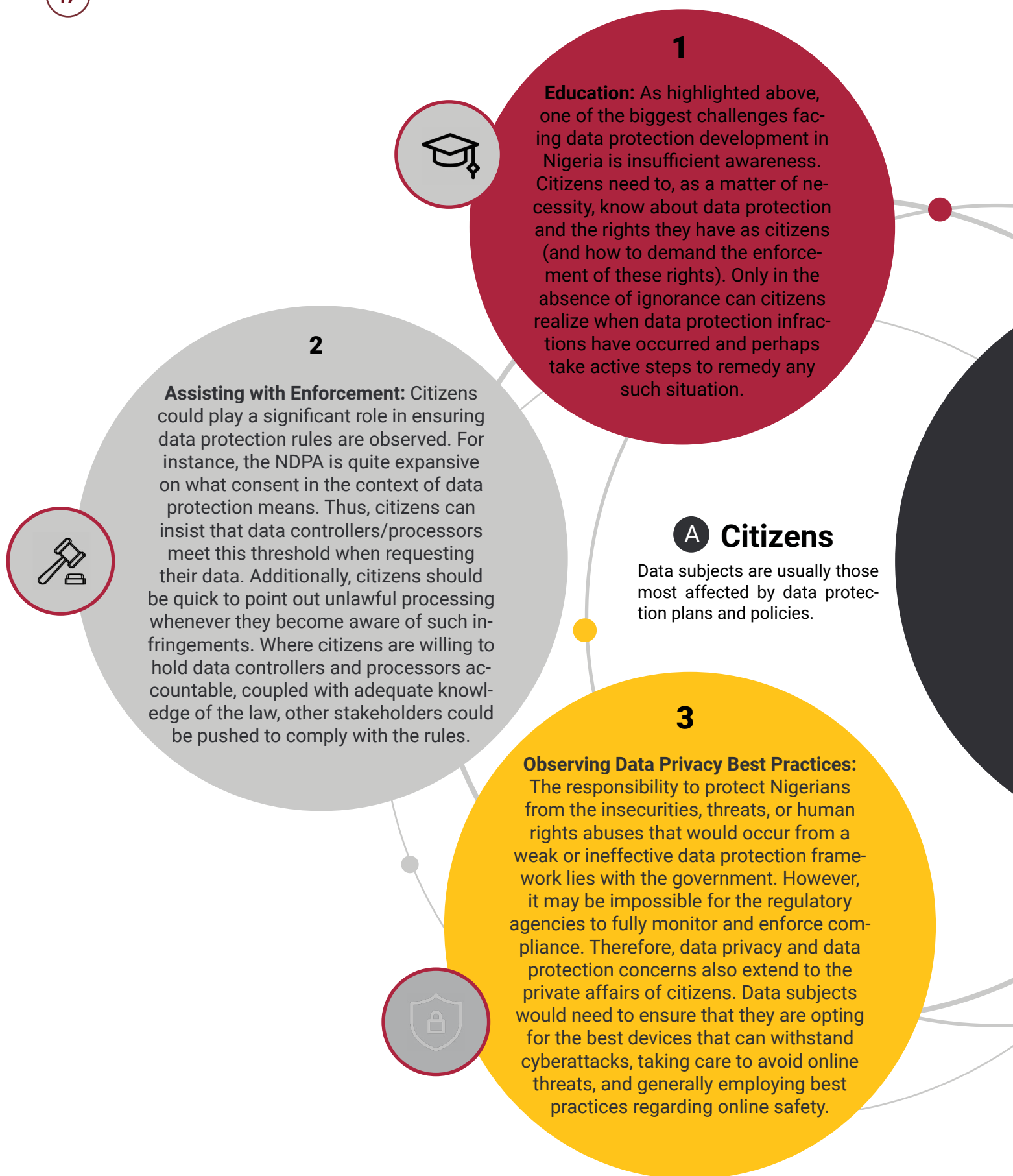


# Policy Takeaway

A consideration of Nigeria's major data protection laws reveals that a wide lacuna has been inadvertently created for law enforcement agencies with minimal accountability and complete freedom from abiding by best practices in data protection, which other public and private institutions are generally bound by. The National Cybersecurity Policy and Strategy 2021 ('the Policy'), issued by the Office of National Security Adviser (ONSA), refers to the enactment of data protection law as a critical component of ensuring national cybersecurity, imperative of internet safety, online protection for children, and gender rights online, it is largely silent on what the ONSA or the agencies under its supervision will do to enhance their data protection practices.

Without compromising the necessity of the highlighted exemptions to fight crime, the absence of accountability measures like data privacy impact assessments denies law enforcement agencies the opportunity for introspection on their methods and the public the ability to hold them accountable. Engagement here should be targeted at securing amendments to extant laws reducing the scope of exemptions, especially with regards to sensitive personal data, providing information on how data is processed (Privacy Policies), and data privacy impact assessments.

Strengthening data protection in Nigeria will take concerted efforts from all stakeholders. This includes regulators, key industry players, and even data subjects (to mention but a few). Below are a few ways data protection could be improved by a few stakeholders:



60 Under the NDPA, where processing is based on consent, it must be demonstrable by the data controller. Consent must be freely and intentionally given, but not through silence, inactivity, or pre-selected confirmations. In determining whether consent was “freely and intentionally” given, consideration will be given to whether the performance of a contract or provision of a service is conditional on consent to processing of personal data that is not necessary for performance of such contract or provision of such service. By implication, where processing is based on consent (and entails performing a contract or providing a service), the data processed should only be data required to perform the contract or provide the service. Consent obtained from data subjects may therefore be provided in writing, orally, or through electronic means. (Section 26 of the NDPA).

## Data privacy principles

Data protection principles serve as fundamental benchmarks in data processing. Every data controller or data processor is expected to abide by these principles when they are engaging in any activity involving the data of natural persons. The principles are:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimization
- Data Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

It is obligatory under data protection regulation to always determine the lawful basis of data processing before embarking on same. There are five lawful bases recognized under the NDPR. They are:

- Consent
- Legal obligation
- Performance of contract
- Vital Interest of the data subject
- Public interest

Any of the above bases is sufficient. Care must be taken by a data controller in choosing its lawful basis because there must be legitimate justification for choosing anyone of the lawful basis.

## Data subject rights

Data Subject rights are essentially integral to the fundamental right to privacy as enshrined under Section 37 of the 1999 Constitution of the Federal Republic of Nigeria. The rights include, but are not limited to the following:

- Right to be informed
- Right to rectification
- Right to access personal information.
- Right to withdraw consent
- Right to be forgotten
- Right to data portability.
- Right to restrict data processing
- Right to object
- Rights in relation to automated decision-making and profiling.

## B Regulatory Bodies

4

### Limiting Legal Interference with Citizen's Data:

If there is a wide room for the government and certain entities to “legally” interfere with citizens’ data, the gains from the Nigerian data privacy regime will never be fully achieved. A definite framework should exist between ensuring national security and upholding data protection rights. Government institutions must be transparent to citizens and accountable to the public for their compliance with and respect for data protection principles in all their endeavours. Regulatory bodies like the NITDA and NCC may need to crucially enforce compliance, including from the government.

5

### Setting Up a Stronger Tech System:

Fighting against data breaches also requires digital and technological sophistication. Unfortunately for the government, on the other side of the fight are experienced hackers and computer experts with systematic understandings of the digital landscape. Besides from making policies and laws, the government needs robust intervention strategies, with *m u l t i d i s c i p l i n a r y* approaches, to improve Nigeria’s tech/digital security infrastructure and improve data protection.

6

### Ensuring that the System Works:

There are various compliance requirements that data controllers and processors have to comply with. To make sure that the law works, the NDPC needs to enforce these compliance requirements. Where the commission lacks the means, systems, and manpower for enhanced monitoring, the government needs to provide same. The laws will only be beneficial to citizens when they are followed by the data controllers, and processors and other stakeholders that the laws regulate.

**Data Privacy Impact Assessment (DPIA):** A DPIA is an entry point to the development and deployment of any tool that requires personal data for its functionalities. A DPIA, as its name suggests, focuses on mitigating risk to privacy including but not limited to analysis of vulnerabilities of data subjects, target results, adverse results, and balancing of data subject rights.

**Data Breach Remediation and Data Protection Compliance Audit:** Data breach remediation is an essential component of data governance. For instance, where there is a breach, a data controller is expected to notify the affected data subject(s) and the regulators of any data breach within 72 hours of becoming aware of the breach. A breach may be an unauthorized access or loss of personal data. There must be a clear policy on disaster recovery and the remedies a data subject may obtain whenever there is a violation of their rights. Also, data processing may require a compliance audit. While it is important for a data controller to set up an audit system internally, an annual filing of compliance audit returns is required. The purposes for conducting an audit include but are not limited to the following:

- To assess the level of compliance with the law
- Evaluate compliance with the organization’s own data protection policy.
- Identify potential gaps and weaknesses in organization’s processes; and
- Give requisite advice and/or remedial actions for identified gaps.

## C The Judiciary

### 7

#### Improving the Status of Data Privacy Rights:

While Nigeria has a fully-fledged process for enforcing the infringement of fundamental human rights, the same cannot be said of digital rights specifically. For anyone to take data privacy rules seriously, the judiciary must show that this right is considered important, and a significant aspect of the human rights of Nigerians. One way to achieve that is by eliminating the so-called dichotomy that may exist between fundamental rights and digital privacy rights.

#### Encouraging the Litigation of Data Privacy Infractions:

### 8

The judiciary should exhibit a willingness to enforce data protection laws through the imposition of appropriate sanctions, as contained in the laws. There is currently a dearth of judicial precedents on data privacy in Nigeria. This is one area in which judicial diligence is required.

### 9

#### Building Expertise Within the Judiciary:

While Nigeria has a fully-fledged process for enforcing the infringement of fundamental human rights, the same cannot be said of digital rights specifically. For anyone to take data privacy rules seriously, the judiciary must show that this right is considered important, and a significant aspect of the human rights of Nigerians. One way to achieve that is by eliminating the so-called dichotomy that may exist between fundamental rights and digital privacy rights.

### Data Sovereignty

A people, through the power entrusted to their own government, have the right to control the data in and/or from their country for the sustainable development of their country. The state sees data as an asset for development planning hence, its capacity to use this asset and protect it as necessity requires cannot be subject to unnatural impediments that may be within or outside the jurisdiction of the State. The government of Nigeria must recognize the importance of data sovereignty in this age of the digital economy. As such, it should commit to ensuring that the data of Nigerian citizens remains under the control of Nigerians as practicable as possible, and that data sovereignty is respected and protected in any international collaborations or partnerships involving the use of such data.



## D Private Sector

10

### Compliance with the NDPA and NDPR

Private sector entities must implement robust data protection measures, including data encryption, secure data storage, and regular audits to ensure the confidentiality, integrity, and availability of personal data. Compliance with the NDPA and NDPR requires private businesses to employ processes that protect personal data lawfully and securely.

11

### Data Protection Officers (DPOs)

Appointing DPOs is essential for compliance with data protection laws. These officers oversee data protection strategies and ensure the company meets legal standards. Related to this, companies should regularly train their employees on data protection best practices and the importance of privacy and security to create a knowledgeable workforce that can proactively protect personal information.

12

### Privacy by Design and Impact Assessments

Integrating data protection into the development and operation of new products, services, and technologies can help in achieving compliance and fostering trust among consumers. Also, conducting regular data protection impact assessments for projects that process personal data helps in identifying risks and mitigating them before they become issues. Organizations should be transparent about their data processing activities, providing clear and accessible privacy policies and notices to individuals whose data they collect.

