African Journal of Legal Research [AJLR] (2026) Vol. 4, No. 7
https://africanjournaloflegalresearch.com [ISSN: 1595 – 5966]

ANALYSING THE EFFECTIVENESS OF THE NIGERIAN DATA PROTECTION LEGAL FRAMEWORK IN ELECTRONIC COMMERCE

Amaayeneabasi Ini Enang*
Ekomobong Ubong Essien**

Abstract

This paper aims to examine the extent of safety of consumers' data in an electronic commerce transaction. Key issues in data processing and protection in electronic commerce were identified to include cross border transfers and third-party risks, risks from data breaches and fraud, consent management overload, amongst others. The Nigerian data protection laws examined include the Nigerian Data Protection Regulation 2019 and the Nigerian Data Protection Act 2023. Similarities between both laws were highlighted as well as notable differences. The Nigerian Data Protection Commission was also examined where successes and enforcement challenges were identified. It was found that the Act does not expressly provide for e-commerce concerns neither does it regulate data selling. This paper makes use of the doctrinal research methodology for its research. This work recommends that the Act should specifically recognise e-commerce peculiarities with regards data processing, especially e-commerce platforms and regulate them accordingly.

Keywords: Data processing, Data protection, electronic commerce, data breaches, Data subjects

1. INTRODUCTION

Data protection has become a top concern globally which has occasioned the enactment of data protection laws across jurisdictions.

* PhD. Email**:** amaayeneabasienang2@gmail.com
** LLM. Email: essieneubong@uniuyo.edu.ng

The need for data protection has been heighted by the digital age where data of data subjects are vulnerable to comprise through cyber security breaches, data selling by data controllers, data damage and data loss. It extends to exposure of bank details on electronic commerce platforms' digital wallets to breaches, data leaks of personal details from health software applications, safety of personal data when users purchase cloud space for data storage.

Nigeria has been in the forefront of regulating and protecting data of data subjects through the enactment of regulations such as the *Nigerian Data Protection Act 2023*, the *Nigerian Data Protection Regulation 2019* and the recent *Nigerian Data Protection Act 2023 General Application and Implementation Directive of 2025* issued by the Nigerian Data Protection Commission which is aimed at implementing the provisions of the NDPA. This new regulation provides notably in article 43[1] which is on emerging technologies that a data processor or controller who deploys or intends to deploy emerging technologies such as artificial intelligence, internet of things and blockchain for the purpose of processing personal data should take into consideration the provisions of the Act, public policy and the GAID. Blockchain technology is also used in electronic commerce to track goods from the manufacturers to the consumers, purchase orders, receipts, amongst others in electronic commerce. It is an immutable ledger. This paper seeks to analyse these laws, regulations and regulatory agencies with the aim of discovering if they have effectively protected data subjects in electronic commerce.

[1] Nigerian Data Protection Act 2023 General Application and Implementation Directive 2025.

2. KEY ISSUES IN DATA PROCESSING AND PROTECTION IN ELECTRONIC COMMERCE

New e-commerce technologies pose fresh technical challenges. Artificial intelligence and machine learning used for recommendation engines and dynamic pricing rely on large datasets and profiling, raising questions about transparency and fairness. For example, the NDPA 2023[2] and the GDPR prohibit solely automated decisions that significantly affect individuals without human intervention, implying firms must provide opt-outs or human review in AI-driven marketing. Meanwhile, Internet of Things (IoT) devices such as smart speakers and wearables may enable e-commerce with voice commands or personalized offers, but they also continuously collect personal data in ways many consumers do not fully understand. Integrating such devices means extending e-commerce data protection to new platforms; any vulnerability in an IoT device or its backend becomes a privacy risk. The GAID's scope as noted earlier extends to AI and IoT but how effective is its implementation?

Cloud computing and third-party services are now ubiquitous in e-commerce for hosting, analytics and payment processing. While cloud infrastructure can improve scalability, it also complicates data jurisdiction and security. Consumer data stored in offshore data centres may be subject to foreign government access or local data-residency mandates. For instance, the NDPA encourages data localization, potentially forcing e-commerce firms to store users' data on local servers. Handling this requires technical solutions such as separate databases, geo-fencing, and constant monitoring of where data replicates. Such measures interact with privacy rules. Furthermore, data flows regularly across national lines through cloud servers, payment gateways, third-party suppliers, etc., as such,

[2] NDPA 2023, s.37.

businesses must navigate varying regimes from the EU's *General Data Protection Regulation* to California's *California Consumer Privacy Act 2020/California Privacy Rights Act 2020* to Canada's *Personal Information Protection and Electronic Documents Act 2000*, Brazil's *General Data Protection Law 2020*, China's *Personal Information Protection Law 2021*, Nigeria's *Data Protection Act 2023* and more in e-commerce, each with distinct definitions of personal data, consent rules, and enforcement mechanisms. This fragmentation creates broad legal challenges, compounded by securing and managing data as well as implementing governance and compliance. [3]

Nigeria's e-commerce faces cybersecurity threats. A global trend is the use of Magecart skimmers to steal payment data. It is a system whereby attackers inject malicious JavaScript into checkout pages to capture credit card details.[4] In 2022, hundreds of Magento-based online stores worldwide including Nigerian sites were compromised to skim payments.[5] There are also cases of large leaks of Nigerian identity and payment data for example online databases selling billions of NIN/BVN records.[6] Such breaches exploit both weak security practices and the secondary market for data in Nigeria.

---

[3] Peter Hall, 'Cross border E-commerce Cybersecurity Challenges', *Secarma* (California,1 February 2024). <https://secarma.com/cross-border-e-commerce-cybersecurity-challenges#:~:text=Cross,but%20also%20about%20navigating%20a> accessed 28 May, 2025.

[4] Prajeet Nair, 'Massive Breach Hits 500 E-Commerce Sites' *Bank Info Security* (10 February 2022) <https://www.bankinfosecurity.com/massive-breach-hits-500-e-commerce-sites-a-18492#:~:text=In%20previously%20reported%20Magecart,by%20security%20firm%20Trend%20Micro> accessed 27 May, 2025.

[5] ibid.

[6] Sylvia Duruson, 'Massive Data Breach Exposes Millions of Nigerians Personal Information' *Tech in Africa* (22 June 2024) <https://www.techinafrica.com/massive-data-breach-exposes-millions-of-nigerians-personal-information/#:~:text=Paradigm%20Initiative%E2%80%99s%20investigation%20rev

E-commerce platforms also struggle with duplicate or inconsistent product entries and missing customer information, leading to order errors, inventory mismatches and poor user experience.[7] Similarly, handling vast volumes of transactions in real time demands low-latency architectures; failures here can lead to cart abandonment and revenue loss[8] as such, ensuring data accuracy and synchronization across multiple channels such as websites, mobile, warehouses is critical but technically challenging. Automated rule engines and geo-tagging are often deployed to enforce region-specific policies. Also, e-commerce operations typically rely on third parties at many stages such as integrating payment gateways, IT providers, and delivery partners. E-commerce platforms share data with multiple vendors, raising liability, privacy and compliance risks[9]. Thus, lack of clear data-processing agreements can expose e-commerce platforms to breaches of local data-protection laws. Traffic spikes for instance flash sales expose limitations in database scaling and message queues, leading to slow page loads and checkout failures.[10] In as much as consumers enjoy tailored product recommendations and dynamic pricing, these practices rely on extensive profiling that seem invasive.

---

ealed%20that,PVC%29%2C%20and%20phone%20numbers> accessed 26 May, 2025.

[7] Vijay Mallik, 'Real-time Data Processing in E-commerce: Challenges and Solutions' (2024) 3(1) IJAETI. <https://ijaeti.com/index.php/Journal/article/view/303?utm_source=chatgpt.com "Real-time Data Processing in E-commerce: Challenges and Solutions"> accessed 25 May, 2025.

[8] ibid.

[9] Gal Ringel, 'E-Commerce Businesses: Five Data Privacy Practices for Gaining Customer Trust In 2022' *Forbes* (New York, 2 February,2022) <https://www.forbes.com/councils/forbestechcouncil/2022/02/02/e-commerce-businesses-five-data-privacy-practices-for-gaining-customer-trust-in-2022/?utm_source=chatgpt.com "E-Commerce Businesses: Five Data Privacy Practices For Gaining ..."> accessed 27 May, 2026.

[10] ibid.

Beyond outright breaches, e-commerce systems face ongoing technical challenges in handling data responsibly. Data mapping is crucial but hard because organizations must know where all consumer data resides. Under laws like NDPA and GDPR, when a data deletion request arrives, controllers must locate and erase the individual's data in all its repositories which could be spread across emails, databases, file servers, and backups.[11] In practice, this is difficult, one breach compliance guide notes that fulfilling a deletion request often means manually searching production and backup environments, a tedious process requiring automation.[12] Without sophisticated data management, enterprises risk non-compliance even absent a breach.

Technical privacy measures such as pseudonymization or anonymization are legally encouraged but themselves challenging. Anonymizing e-commerce analytics while still providing personalized service is technically complex. Moreover, some laws require data minimization which involves only collecting what is strictly needed, this can conflict with e-commerce trends toward data-rich personalization. Implementing data minimization means re-engineering platforms to avoid storing unnecessary data fields for example tracking consumer metrics in aggregate rather than per individual, which requires careful design. Inadequate handling can lead to regulatory breaches or consumer distrust. As Moric pointed

[11]A. Lonzetta, 'Challenges of Complying with Data Protection and Privacy Regulations' (2020) EAI <https://www.researchgate.net/publication/346886893_Challenges_of_Complying_with_Data_Protection_and_Privacy_Regulations#:~:text=O%20rganizations%20need%20to%20have,clear%20unders%20tanding%20of%20their> accessed 27 May, 2026.
[12] ibid.

out, e-commerce growth often exposes personal data to potential cyber threats and trust can suffer when data is used opaquely.[13]

E-commerce platforms must guard against cyber threats that endanger personal data as noted earlier. By nature, online retailers collect sensitive consumer details including names, addresses, payment info, purchase history, making them attractive targets for hackers. Threats include website hacking, malware injection into third-party payment scripts for instance, phishing, and insider misuse. A lack of timely security updates or misconfigured systems can lead to large-scale breaches. The resulting consequences are severe. In cross-border e-commerce, breaches can be especially problematic for instance, a vulnerability on a Nigerian-hosted site selling internationally may trigger enforcement under EU/GDPR standards if EU residents are affected.[14]

Furthermore, privacy laws rarely prescribe specific technologies, leading to ambiguity in technical compliance. As Lonzetta notes, many data protection regulations mandate security controls which could include encryption, data anonymization or pseudonymization, and access/identity management, however, the regulations do not identify specific controls.[15] This open-ended requirement forces companies to interpret and choose appropriate measures themselves. In addition, companies face divergent enforcement challenges. For instance, a breach may trigger proceedings under multiple laws involving class actions under United States law for example and fines under the NDPA. Courts may also diverge in interpreting statutes. Liability can

[13] Zlatan Moric, 'Protection of Personal Data in the Context of E-Commerce' (2024) JCSP 4(1). <https://www.mdpi.com/2624800X/4/3/34#:~:text=Like%20many%20other%20regions%2C%20Croatia,This%20is> accessed 27 May 2026.
[14] ibid 34.
[15] Lonzetta (n 11), 118.

thus multiply and one breach can lead to compound penalties worldwide.

3. NIGERIAN DATA PROTECTION REGULATION 2019

The Nigerian Data Protection Regulation (NDPR) 2019 is a regulatory framework established to protect the privacy rights of individuals and to regulate the processing of personal data in Nigeria. Its objectives include 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 through the safe-guards afforded by a just and equitable legal regulatory framework on data protection that is in tune with best practices. In 2020, the Nigerian Data Protection Regulations Implementation Framework, was issued by the National Information Technology Development Agency (NITDA) to clarify provisions of the NDPR and relevant laws applicable to it.

The significance of data protection regulations in e-commerce arises from the acquisition of sensitive information related to customers during business transactions, such as delivery addresses, bank details, and personal identification. Additionally, in e-contracting, regulations are relevant due to the presence of click wrap and browse wrap agreements, which frequently contain cookies and third-party cookies. These agreements often include provisions that allow for the utilization and sharing of user data, including browsing histories of individuals who browse websites.[16]

[16]A Afolabi, 'Data Protection Regulation and Implications for Data Privacy in Nigeria'. JCP 1(1) 53-64. <https://doi.org/10.1007/s42455-020-00008-6> accessed 28 April 2026.

The Regulation applies to all transactions involving the processing of personal data notwithstanding how the data processing is conducted, and to all-natural person's resident in the country as well as Nigerians residing abroad. The extension of the application of the regulation to the protection of personal data of Nigerian citizens residing outside the country's territory raises the question of enforceability.[17]

The Regulation defines personal data as any information relating to an identified or identifiable natural person, who is considered a data subject.[18] Anyone entrusted with or in possession of personal data owes a duty of care to the data subject and is accountable for his or her acts or omissions in respect of data processing under the principles contained in the regulation which are highlighted in the following paragraphs.[19]

On lawful processing of data, the foremost principle of data processing is that processing of data must be for legitimate purposes and must be fair. Processing of data is lawful if it meets at least one of the conditions set down in Part 2.2 of the Regulations, which include the data subject's consent to the processing of his or her personal data for one or more specific purposes,[20] for example, the performance of a contract to which the data subject is a party or steps taken at the request of the data subject prior to entering into a contract.[21] Consequently, processing of personal data in all forms of commercial transactions in which consumers daily engage in, including e-commerce, qualifies as lawful purpose under the regulation. Even, personal data of a consumer collected while window shopping on the

[17]D Igegbulem, O Ukwueze, 'Deconstructing Nigeria's Data Protection Regime from Consumer Protection Perspective. (2021) 13(1) *TLSTR* 94-118.
[18] NDPR Part 1.3(r)
[19]Ibid 98.
[20]NDPR Part 2.2(a)
[21]NDPR Part 2.2(b)

internet will satisfy the requirement of lawful purpose since such a visit to the website of an undertaking is a necessary preliminary to entering into a transaction with the undertaking.[22]

On procuring consent, part 2.3 provides that personal data shall not be obtained except if the specific purpose of the collection is made known to the data subject and his or her consent is obtained without fraud, coercion, or undue influence. Similarly, browse wrap contracts most times bind the user whether he consents to the contract or not so long as the user uses the browser or opens the website link. By inference, Part 2.2(a) deems the above act as unlawful.

On data privacy and security, anyone involved in the control of the processing of personal data is mandated to develop security measures to protect such data. The prescribed measures include, but are not limited to, protecting systems from hackers, setting up firewalls, storing data securely with access to specific authorised individuals, employing data encryption technologies, developing organisational policy for handling personal data and other sensitive or confidential data, protecting emailing systems and continuous capacity building for staff.[23]

3.1 Rights of Data Subjects

Data subjects have rights provided for and protected under the *Nigerian Data Protection Regulations 2019*. Some of the rights include;

[22]T Abimbola & A Oluwaseun. 'Data Protection Regulation and Cyber Security in Nigeria'. (2021) JISC 1(1) 31-42. < https://doi.org/10.47750/jisc.v1i1.32> accessed 28 April 2026.
[23]NDPR Part 2.6.

3.2 Rights to Information

Data subjects have the rights to information relating to the collection, processing, storage, and transfer of their personal data. Privacy policies are to contain information such as what constitutes the data subject's consent; a description of collectable personal information; the purpose of collection of personal data; and technical methods used to collect and store personal information, cookies, web tokens, etc.[24]

3.3 Right to Erasure of Personal Data and Information or Right to be Forgotten

A data subject has the right to request the controller to delete his or her personal data and the controller shall comply without delay, especially where these data are no longer necessary considering the purposes for which they were collected or processed. Other grounds on which a data subject's right to request deletion of data include where the data subject withdraws consent on which the processing is based; the data subject objects to the processing and there are no overriding legitimate grounds for the processing; the personal data have been unlawfully processed; or the personal data must be erased for compliance with a legal obligation in Nigeria. In any case, the particular controller who has made the personal data public and is obliged to delete the personal data shall take all reasonable steps to inform other controllers processing the personal data of the data subject's request.[25] The right of erasure is also known as the right to be forgotten and is also available under the EU's General Data Protection Regulation.[26]

3.4 Right to Restrict Processing of Personal Data

A data subject can ask the controller to restrict processing of their personal data if any of these apply:

---

[24]NDPR Part 3.1(1)
[25]NDPR Part 3.1(9)(10)
[26]General Data Protection Regulation 2018 (GDPR), a.17 and 19

a. They contest the data's accuracy while the controller verifies it.
b. The processing is unlawful and they prefer restriction instead of erasure.
c. The controller no longer needs the data but the data subject needs it for legal claims.
d. They object to processing while it's being determined whether the controller's grounds override theirs. [27]

When processing is restricted, the data may only be stored and otherwise processed only with the data subject's consent, for legal claims or to protect another person's rights, or for important public interest in Nigeria.[28]

3.5. Right to be Notified of Rectification, Erasure or Restriction of Personal Data

The data controller is obligated to communicate any rectification, erasure of personal data or restriction to each recipient to whom the personal data has been disclosed unless this proves impossible or involves disproportionate effort. In that case, if the data subject requests, the controller shall inform him or her about those recipients.[29]

Another right available to a data subject is the right to receive and transmission of personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used machine-readable format. A data subject also has the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where the processing is based

[27]NDPR Part 3.1(11)
[28]NDPR Part 3.1(12)
[29]NDPR Part 3.1(13)

on consent or contract, and the processing is carried out by automated means.[30]

The Regulation does not prescribe any mitigating measures that can be adopted on the occurrence of personal data breach. This omission is not peculiar to the Regulation but is noticeable in even seemingly extensive data protection laws including the EU's General Data Protection Regulation.[31]

The Regulation prescribes penalties for default ranging from ₦200,000 to ₦10 million[32] as well as imprisonment terms,[33] and any breach of the regulation shall be construed as a breach of the provisions of the *National Information Technology Development Agency Act* 2007.[34]

4. CHALLENGES OF THE NIGERIAN DATA PROTECTION REGULATION 2019

In addition to the challenges earlier noted, compliance with the NDPR can be a significant challenge for companies, particularly smaller ones that may not have the resources to implement the necessary data protection measures. There are concerns that some companies may ignore the regulation or only implement superficial measures to comply with it.[35]

[30]NDPR Part 3.1(14)
[31]D Igegbulem, O Ukwueze, 'Deconstructing Nigeria's Data Protection Regime from Consumer Protection Perspective. (2021) 13(1) TLSTR 99.
[32]NDPR Part 2.10
[33]NITDA Act, ss. 17 and 18.
[34]NDPR Part 4.2(6)
[35]T Oyegoke, & O Babalola 'Data Protection Regulation and Cloud Computing Adoption in Nigeria: A Conceptual Framework'. (2020). *Journal of Cybersecurity Research*, 2,1, 23-38. <https://doi.org/10.22059/jcsr.2020.303827.1008007> Accessed 28 April 2026.

The NDPR requires that companies ensure that any personal data transferred outside of Nigeria is done in compliance with the regulation and any other relevant laws and regulations. However, this can be a challenge in the context of electronic commerce transactions, where data may be transferred across borders frequently. Moreover, despite the NDPR's focus on data protection, data breaches can still occur, exposing consumers' personal data to unauthorized access.[36]

Most importantly, the Regulation does not recognize nor make any reference to electronic commerce, nor protection of consumers data in online payment systems, nor cloud computing concerns, nor data selling in electronic commerce.

4.1 The Nigeria Data Protection Act, 2023

The Nigeria Data Protection Act, 2023 provides a comprehensive legal framework for the protection of personal information. The Act aims to safeguard the fundamental rights and freedoms of data subjects, ensure fair and lawful processing of personal data, and establish a regulatory body to supervise data protection. It applies to any processing of personal data by data controllers or processors domiciled or operating in Nigeria, or when the data subject is in Nigeria.[37] Notably, the NDPA's extraterritorial scope means that any processing of a Nigerian's personal data, even by controllers or processors without any Nigerian presence, falls within the law[38]. In practice, this means both local e-commerce platforms for instance Jumia, Konga, and foreign platforms for instance, Chinese's Temu and America's Amazon targeting Nigerian consumers must comply with the NDPA when

[36]O Adebayo & S Adeniyi 'Understanding the Nigerian Data Protection Regulation 2019: A Review of Its Legal and Regulatory Implications'. (2020). *Journal of Law, Technology and Policy* 1,1, 11-20. <https://doi.org/10.47750/jltp.v1i1.7> Accessed 28 April 2026.
[37] Nigeria Data Protection Act 2023, Part I.
[38] Part viii.

handling Nigerians' data. The Act also incorporates novel obligations such as a statutory duty of care on processors/controllers, and requires controllers to engage accredited Data Protection Compliance Organizations.

The Act establishes the Nigeria Data Protection Commission, an independent regulatory body with the authority to oversee the implementation of data protection laws, register data controllers and processors, and promote public awareness of data protection rights.[39] It outlines principles for processing personal data, including fairness, transparency, data minimization, accuracy, and security. It specifies lawful bases for data processing, such as consent, legal obligation, public interest, and legitimate interests.[40]

On rights of a data subject, data subjects have rights including access to their data, correction and erasure, data portability, the right to object to data processing, and withdrawal of consent.[41] For example, any e-commerce site collecting payment or delivery details must notify buyers/consumers the reason the data are needed and cannot use it beyond that purpose. On data security, data controllers and processors must implement appropriate technical and organisational measures to ensure the security, integrity, and confidentiality of personal data,[42] security measures may include encryption, access controls, firewalls, etc. Controllers must process data only on lawful bases through for example consent, contract necessity, legal/public interest, vital interests, or legitimate interests, though the NDPA places tighter limits on legitimate interests than the NDPR. For sensitive personal data such

[39] Part II.
[40] Part v.
[41] Part vi.
[42] Part vii.

as financial, health, religious data, the NDPA generally requires explicit consent.

On enforcement, the Commission is empowered to handle complaints, conduct investigations, issue compliance and enforcement orders, and impose penalties for non-compliance with the Act.[43] The Act is a significant step in enhancing data privacy and protection in Nigeria, providing a clear legal framework and establishing a regulatory authority to enforce compliance and safeguard data subjects' rights.

4.1.1 Obligations on Local and Foreign Platforms

As earlier noted, foreign platforms even without Nigerian offices fall under the NDPA's extraterritorial clause by virtue of section 2(2)(c). Thus, any processing of a Nigerian's data by an entity not established in Nigeria is covered.[44] In effect, a United States or Chinese e-commerce site targeting the Nigerian market is legally required to abide by NDPA standards.

Concretely, controllers must obtain valid consent or another legal basis before collecting personal data, and they must give consumers notice for instance through privacy policies that explains the purpose of collection and any onward transfer. The NDPA's processing principles in Section 24 require that data be handled fairly, lawfully and transparently and that controllers demonstrate accountability and a statutory duty of care.[45] High-risk processing such as profiling or large-scale use of sensitive data triggers additional requirements like Data Protection Impact Assessments. Controllers of major importance

[43] Part x.
[44] Mercy King'ori, 'Nigeria's New Data Protection Act Explained' *Future of Privacy Forum* (Lagos, 28 June 2023) <https://fpf.org/blog/nigerias-new-data-protection-act-explained/#:~:text=Section%202,which%20include%20the%20%E2%80%9Ctargeting%E2%80%9D%20criteria> accessed 28 May 2025.
[45] Ibid

perhaps, for instance very large e-commerce platforms must register with the NDPC and appoint a Data Protection Officer. Every processor not excluding third-party information technology vendors must contractually ensure NDPA compliance.

Critically for cross-border e-commerce, the NDPA restricts transfers of Nigerian data abroad as earlier noted. Outbound transfers are only permitted if the destination country has been declared adequate by Nigeria or if appropriate safeguards are in place. Otherwise, transfers require individual exceptions for example explicit consent of the consumer, contract necessity, public interest, legal claims, or vital interests.[46]

4.1.2 Similarities Between Nigeria Data Protection Regulation 2019 and Nigeria Data Protection Act 2023

There are several similarities between the *Nigerian Data Protection Regulation* (NDPR) 2019 and the *Nigerian Data Protection Act* (NDPA) 2023. The NDPR 2019 served as Nigeria's initial framework for data protection and laid the groundwork for the more comprehensive NDPA 2023. Firstly, both the NDPR 2019 and the NDPA 2023 are built around fundamental principles of data protection, such as lawfulness, fairness, transparency, data minimisation, accuracy, storage limitation, and integrity and confidentiality. These principles guide how personal data should be processed to protect the rights of individuals.

Secondly, both regulations outline specific lawful bases for processing personal data. These bases include consent of the data subject,

[46] 'Data Protection Laws in Nigeria' *DLA Piper Intelligence* (Abuja, 18 January 2025) <https://www.dlapiperdataprotection.com/?c=NG&t=law#:~:text=In%20the%20absence%20of%20adequacy,the%20following%20conditions%20are%20met> accessed 27 May 2025.

performance of a contract, compliance with a legal obligation, protection of vital interests, performance of a task carried out in the public interest, and legitimate interests pursued by the data controller or a third party.

Furthermore, both the NDPR 2019 and the NDPA 2023 grant data subjects' similar rights, such as the right to access personal data, the right to rectify inaccurate data, the right to erasure (also known as the right to be forgotten), the right to restrict processing, the right to data portability, and the right to object to data processing.

In addition, both the NDPR and the NDPA regulate the transfer of personal data outside Nigeria. Transfers are permitted only when the receiving country has adequate data protection standards, or when specific conditions are met to ensure that data subjects' rights are not undermined.

Also, both frameworks require data controllers and processors to implement appropriate technical and organisational measures to protect personal data against unauthorised access, alteration, and loss. They also impose obligations to report data breaches to the relevant authorities and, in certain circumstances, to the affected data subjects.

Furthermore, the NDPR 2019 and NDPA 2023 both outline obligations for data controllers and processors, including the need for privacy policies, proper data management practices, and adherence to data protection impact assessments for high-risk processing activities.

Lastly, both frameworks emphasise the importance of obtaining valid consent from data subjects before processing their personal data. This includes ensuring that consent is specific, informed, unambiguous, and freely given.

4.3 Notable Differences

While there are similarities, the NDPA 2023 introduces several enhancements and expansions to the regulatory framework to include first, on establishment of the Nigeria Data Protection Commission (NDPC), the NDPA 2023 establishes the Nigeria Data Protection Commission as the regulatory authority responsible for enforcing data protection laws, while the NDPR 2019 was implemented under the supervision of the National Information Technology Development Agency (NITDA).

Secondly, on a comprehensive legal framework, the NDPA 2023 is a more comprehensive and detailed legal framework that covers a broader range of issues and introduces specific obligations, penalties, and enforcement mechanisms, compared to the NDPR 2019, which was more of a guideline.

Lastly, the NDPA 2023 provides the Commission with enhanced enforcement powers, including the authority to conduct investigations, impose fines, issue compliance notices, and prosecute offenders, while the NDPR 2019 mainly relied on NITDA's administrative capabilities.

4.4 Critique of the Nigeria Data Protection Act 2023

The Nigeria Data Protection Act 2023 (NDPA) is a significant step forward in safeguarding personal data and privacy rights in Nigeria. It establishes the Nigeria Data Protection Commission (NDPC) as the regulator and provides a legal framework for data protection. However, while the Act has been welcomed for its comprehensive approach to data protection, there are several areas where it faces criticism which will be discussed below.

4.4.1 Electronic Commerce and Cloud Computing Concerns

Similar to the Nigerian Data Protection Regulations, the NDPA does not recognize nor regulate electronic commerce concerns earlier identified in this paper. It does not also provide for protection of e-commerce consumers' data in online payment systems, nor make mention of contingency plans to be put in place in event of data and cyber security breaches. It does not provide for cloud computing concerns especially prohibiting cloud service providers from excluding themselves from liability for loss, breach, or damage of stored data by cloud service providers. It does not also prohibit them from using stored consumers data and purchase patterns for targeted advertising. It does not also regulate data selling between social media platforms and e-commerce platforms in electronic commerce.

4.4.2 Heavy Reliance on Consent

The NDPA 2023 heavily relies on consent as the primary basis for data processing. While obtaining consent is a cornerstone of data protection, over-reliance on it can lead to consent fatigue where e-commerce consumers routinely accept terms without fully understanding the implications. This approach may not always provide the best protection for data subjects, especially in situations where there is an imbalance of power between the data controller and the data subject.

4.5 Nigeria Data Protection Commission

The enforcement of the Nigeria Data Protection Act (NDPA) of 2023 and the Nigerian Data Protection Regulation (NDPR) of 2019, falls under the jurisdiction of the Nigeria Data Protection Commission (NDPC), formerly known as the Nigeria Data Protection Bureau (NDPB).

The NDPC is empowered to do the following.

a) Monitor and enforce compliance with the provisions of the NDPR and NDPA.
b) Investigate data breaches and complaints from data subjects (individuals) concerning the misuse of their personal data. NDPC currently collaborates with National Information Technology Development Agency (NITDA), Federal Competition and Consumer Protection Commission (FCCPC), Nigerian Communications Commission (NCC), Independent Corrupt Practices and Other Related Offences Commission (ICPC), Economic and Financial Crimes Commission (EFCC) and the Nigeria Police Force (NPF) to carry out its investigative powers over data controllers and data processors for various degrees of data privacy and protection breaches.[47]
c) Impose penalties and fines for violations, ensuring organizations adhere to the regulations.
d) Audit data controllers and processors to ensure they have the necessary measures in place for the protection of personal data.

It should be noted that the *Cyber Crimes Amendment Act 2024* introduced the requirement for service providers to coordinate with their respective sectoral Computer Emergency Response Teams (CERTs) or sectoral Security Operations Centres (SOC) through a Coordination Centre, enhancing collaboration in handling cyber incidents.[48] Furthermore, the time frame for reporting incidents is now 72 hours of its detection,[49] no longer 7 days as contained in the 2015 Act. This change emphasizes the importance of prompt reporting and

[47] *National Data Protection Commission News* <https://www.ndpc.gov.ng/Home/NewsDetails/23> accessed 28 October 2025.
[48] Cybercrimes Act, s. 21(1)(a).
[49] Cybercrimes Act, s. 21(1)(b).

response to cyber incidents for effective mitigation and prevention of cyber threats.

This reporting provision is also in line with the data breach reporting requirements of the NDPA, which compel reports of data breaches within 72 hours of becoming aware of the data breach. Although the NDPA already covered the ambit of data breaches, cyber incidents are wider than data breaches and may or may not include data breaches. For example, a cyber incident may cause network outages or disruptions, and during that network disruption, data may not be breached or stolen. Hence, where there is a cyber incident, the report should be made in accordance with the *Cybercrime Act* and the NDPC should be informed where there is a data breach during the cyber incident.

Furthermore, the NDPC is also tasked with overseeing data protection compliance frameworks in both the public and private sectors, ensuring that businesses, government agencies, and other entities adhere to globally recognized standards of data privacy and protection.

4.5 Enforcement Challenges

While the Nigerian Data Protection Act and Regulation represent significant strides toward safeguarding data privacy, their enforcement has faced mixed results due to several challenges and limitations.

a. Limited Resources and Capacity: The NDPC, like many regulatory bodies in Nigeria, faces challenges with funding, staffing, and technology. With data processing growing rapidly across sectors like finance and healthcare, the NDPC's resources are stretched thin, limiting its capacity to audit all organizations and enforce

compliance consistently.[50] In *Babalola v Minister of Communications, Innovation and Digital Economy & 5 Ors*,[51] the plaintiff sued the defendants for failure to fund the NDPC.

b. Inconsistent Compliance Across Sectors: While larger corporations in sectors such as telecommunications and finance have made efforts to comply with data protection laws, many smaller organizations, particularly in the informal sector, lack the resources or incentives to comply. This creates an uneven playing field in data protection enforcement.
c. Non investigation of Electronic Commerce Businesses: NDPC has been more focused on other sectors but fail to investigate e-commerce businesses for data breach. For example, in December 2023, Jumia, a leading Nigerian e-commerce platform, suffered a significant data breach, exposing the personal details of customers. While the breach highlighted the importance of robust data security measures, enforcement actions against the company were slow. The NDPC's response was criticized for not being immediate or strong enough, reflecting weaknesses in rapid incident response capabilities.[52] In November 2023, Flutter wave, a Nigerian fintech company which partners with e-commerce service providers including Multichoice disclosed a data breach that exposed the personal information of its customers. The breach included names, email addresses, and phone numbers. Despite being audited by NDPC, Flutter wave was not investigated nor fined for the

[50] I Peters, 'NDPC Funding: NASS Counters Olumide Babalola's Suit, Argues Jurisdiction, Applicant's Locus Standi' (DNL Legal and Style, 21 September 2024) <https://dnllegalandstyle.com/dnl/ndpc-funding-nass-counters-olumide-babalolas-suit-argues-jurisdiction-applicants-locus-standi> accessed 28 October 2024.
[51] FHC/LF/41/2024 (Unreported)
[52] Info Security 'Experian South Africa Breach' <https://www.infosecurity-magazine.com/news/experian-south-africa-breach/> accessed 28 October 2024.

breach.[53] Conversely, in other jurisdictions such as the UK, the Information Commissioner's Office fined British Airways £20 million under the GDPR for a consumer-data breach when the ticket was purchased online. Similarly, in the U.S. in 2022, beauty retailer Sephora agreed to pay $1.2 million to settle CCPA violations after failing to inform consumers that it sold their personal data and not honouring opt-out requests.[54]

5. FINDINGS

This work finds that many e-commerce entities lack robust encryption, secure payment gateways, strong authentication, and incident-response/contingency plans. In addition, data controllers and cloud providers sometimes use or sell user data (including via buried contract clauses), increasing the risk of privacy harm. Also not included in the laws are clear rules for cloud service providers including prohibition of exclusions of liability clauses in standard contracts with e-commerce consumers nor is strict liability imposed on them for sale, loss, or damage to stored data.

Lastly, the NDPC lack sufficient funding and trained staff to respond quickly and effectively to breaches and to oversee emerging technologies. The absence of a specialised joint task force with the Cybercrimes (Amendment) Act's implementation agencies for

[53] J Uzoma, 'African Fintech Firm Flutter Wave Confirms Data Breach' (TechCrunch, 18 November 2023) <https://techcrunch.com/2020/11/18/african-fintech-firm-flutterwave-confirms-data-breach/> accessed 28 October 2024.

[54] Sarah Merken, 'Sephora to Pay $1.2 Million in Privacy Settlement with California AG Over Data Sales' *Reuters* (Boston, 2 August 2022). <https://www.reuters.com/legal/litigation/sephora-pay-12-mln-privacy-settlement-with-calif-ag-over-data-sales-2022-08-24/#:~:text=%28Reuters%29%20,said%20in%20a%20Wednesday%20statement> accessed 2 May, 2025.

instance, the Computer Emergency Response Teams (CERTs), makes implementation of the NDPA difficult.

6. CONCLUSION

Data protection in electronic commerce remains a very delicate issue in Nigeria and around the world. The Nigerian data protection framework provides a foundational structure for safeguarding personal data in electronic commerce, with clear rights for data subjects, obligations for controllers, and mechanisms for enforcement. However, gaps remain including limited enforcement capacity, inconsistent compliance across businesses, unclear sector-specific guidance, not providing for cloud computing issues and challenges in cross-border data transfers undermine its full effectiveness.

7. RECOMMENDATIONS

In as much as we have a robust legal regime on data protection, enforcement still remains an issue. Thus, companies must ensure to have security measures including robust encryption, secure payment gateways, and strong authentication measures put in place as well as contingency plans data breaches occur, these are essential in protecting consumer data in e-commerce. Data controllers should ensure to guard against selling data of data subjects. NDPC should be well funded to effect quick responses to breaches. Its staff must be adequately trained in the use of emerging technologies to aid smooth operations. The NDPA should specifically provide for electronic commerce as well as data protection in the digital space for example cloud service providers. It should specifically prohibit them from excluding themselves from liability for loss, breach damage of stored data by cloud service providers.

Cloud Service Providers must protect users stored data from unauthorised access, including access by foreign governments,

whether formally demanded or not. In addition, cloud service providers should refrain from using stored data for other purposes such as selling them to commercial companies for advertisement purposes. Companies like Google and Amazon for instance, have been scrutinized for using data from their cloud services for targeted advertising.[55] Google has been known to analyse data from Gmail and other services to provide more personalized advertisements.[56] While the data may be anonymized, there are still risks of re-identification, leading to privacy concerns. Moreover, many cloud service providers include clauses in their terms and conditions that allow them to use or share user data with third parties. Often, these clauses are buried in lengthy legal documents that users might not read thoroughly.[57]

The NDPA should therefore impose strict liability and penalties on cloud service providers with regards breach, unauthorised access, selling, loss and damage of data of users stored in their cloud space. Lastly, there should be a joint task force comprising the Cybercrimes' Computer Emergency Response Teams and the NDPC to ensure effective response to data breaches and issues generally.

[55] R. Feldman, 'Google and Facebook's Hidden Data Deal That Hides Ads from the Public' *Example* (Washington, 5 July 2021) <https://www.example.com> accessed 9 August 2024.
[56] Ibid
[57] P Macdonald, 'Legal Analysis of Data Monetization Practices in Cloud Services', (2022) JCCL 23(2) 89-110.