

Analysis of the Nigerian Data Protection Act 2023 and the Regulatory Framework for Fintech in Nigeria: Towards a Cohesive Regime

Osilojo, O. Olumayowa Esq* and Oyeleke S. Oyeniran, Esq**

ABSTRACT

The Nigerian Data Protection Act (NDPA) 2023 represents a significant milestone in the evolution of data privacy regulations in Nigeria, particularly for the fintech sector, which handles vast amounts of sensitive personal and financial data. This paper compares the Act with its immediate predecessor, the Nigerian Data Protection Regulation (NDPR) 2019, and with the benchmark EU General Data Protection Regulation (GDPR). The essence of this comparative analysis is threefold: first, to identify the substantive legal improvements introduced by the NDPA 2023; second, to highlight remaining regulatory gaps relevant to the fintech sector; and third, to assess Nigeria's level of convergence with internationally accepted data protection principles. The paper further examines the doctrinal implications of the NDPA's provisions for fintech companies, emphasising the operational and reputational necessity of compliance. It also addresses key challenges to the Act's implementation, including vague terminology, limited public awareness, and a shortage of trained data protection professionals. By acknowledging these advancements and obstacles, the study concludes with targeted recommendations for enhancing data literacy, clarifying regulatory requirements, and strengthening enforcement with the aim of ensuring robust data protection within Nigeria's rapidly growing fintech industry.

Keywords: Data Protection, Fintech, Privacy regulation, Nigerian Data Protection Act 2023 and Compliance

1.0 INTRODUCTION

The rise of fintech in Nigeria started from mobile payments, it has now evolved to a more sensitive regime like digital lending and other financial top risks. The evolvment has unlocked unprecedented financial inclusion, yet it has simultaneously created a vast new frontier of sensitive personal data ripe for exploitation¹. To understand the scope of this new

¹ Udosen Jacob Idem and others, 'Data Privacy and Protection Laws in Nigeria for Sustainable Development: Insights from International Perspectives' (Conference Paper, 2024 IEEE 5th International Conference on Electro-Computing Technologies for Humanity (NIGERCON), November 2024).

regime, it is essential to ground the discussion in what data protection entails. David Millard defines Data Protection as the process of safeguarding personal information from unauthorized access, use, disclosure, alteration, or destruction.² Christopher Kuner in the same vein posited that "Data protection involves the establishment and enforcement of rules and procedures aimed at controlling and managing the collection, storage, processing, and transfer of personal data, with the goal of ensuring individuals' privacy rights are respected³. Data protection has been an essential concern throughout human history, even in the earliest civilizations⁴. It gained popularity worthy of legal protection as a result of the article written by the two American lawyers, Samuel D. Warren and Louis Brandeis⁵." They were concerned about the growing intrusion into people's private lives, especially with the rise of technologies like photography and newspapers. They argued that individuals should have legal protections against unwarranted publicity and intrusion into their personal affairs⁶. This article sparked global discussions about privacy and laid the foundation for modern privacy laws⁷. It also influenced the inclusion of the right to privacy in the Universal Declaration of Human Rights in 1948⁸. This declaration set a standard for countries around the world to protect the privacy rights of their citizens.

The advent of the internet in the 1970s brought new challenges to privacy⁹. With the internet, personal data could be easily accessed and exploited by malicious actors. Cookies, for example, allowed websites to track users' behaviour and preferences, raising concerns about data privacy and security. Today, data protection is more important than ever as we navigate the digital age. Laws and regulations continue to evolve to address new threats and challenges, but the fundamental principles of privacy remain constant. Beyond several National Legislation that address Data Protection menace, several continental bodies have enacted laws about data protections¹⁰. Some of them are Africa Union Convention on Cyber

² Millard, D., & Walden, I. (2018). *Data Protection: A Practical Guide to UK and EU Law*. Oxford University Press

³ Kuner, C. (2012). *European Data Protection Law: Corporate Compliance and Regulation*. Oxford University Press

⁴ A Brief History of Data Protection: How Did It All Start?' (INPLP, 1 June 2018) <https://inplp.com/latest-news/article/a-brief-history-of-data-protection-how-did-it-all-start/> accessed 1 May 2025

⁵ Tadesse Biru Kersmo, 'The Right to Privacy: A Reflection on Warren and Brandeis' Interpretation and the Case of Ethiopia 1991–2018' (2022) 4(4) *International Journal of Arts, Humanities and Social Studies* 120.

⁶ Ibid.

⁷ Cite works or publications that support this assertion otherwise, it is mere assumption.

⁸ Cite the specific article of the UDHR touching on privacy.

⁹ Sources?

¹⁰ Examples should be given as footnote.

Security and Personal Data Protection, Economic Community of West African States (ECOWAS) Supplementary Act on Personal Data Protection 2010, European Union (EU) General Data Protection Regulation (GDPR), etc. This article is motivated by the tension between innovation and privacy in Nigeria's rapidly expanding fintech sector. Its aim is to conduct a doctrinal appraisal of the applicable data regulation framework (notably the Nigeria Data Protection Act, 2023) to determine whether it provides sufficient legal clarity and robust safeguards. The appraisal seeks to articulate clear recommendations for regulatory enhancement to foster a trustworthy and competitive digital finance ecosystem.

2.0 FINTECH AND DATA PROTECTION

Fintech are the categories of companies that use technological tools to provide financial solutions using internet and automated tools¹¹. Prior to evolution of fintech regime, banking system has used analogue tools to conduct their banking system, fintech has proven to be faster, reliable and easier to use¹². Fintech innovations have consistently disrupted the financial services sector by offering products and services that were previously exclusive to traditional banks prior to the financial crisis of 2008 and the pandemic crisis of 2010¹³. In a similar vein to traditional banks, it is imperative to regulate the Fintech sector to mitigate potential risks that can affect individuals across various economic strata, regardless of their level of development¹⁴. In recent years, there has been a significant expansion in the financial technology sector, characterized by a proliferation of products and services. These offerings encompass a wide range of consumer-oriented platforms, including brokerages that prioritize user experience, automated investment advisors, lending platforms, mobile payment applications, and platforms facilitating cryptocurrency trading. Fintech enterprises inherently

¹¹ Zakia Siddiqui and Claudio Andres Rivera, 'Fintech and Fintech Ecosystem: A Review of Literature' (2022)

¹² Risk Governance and Control: Financial Markets & Institutions 63

¹² Ross P Buckley, Douglas W Arner and Janos Nathan Barberis, 'The Evolution of Fintech: A New Post-Crisis Paradigm?' [2016] SSRN Electronic Journal <https://doi.org/10.2139/ssrn.2676553>.

¹³ Usoro Usoro, Impact of Technology on Financial Services (Research Paper, Central Bank of Nigeria 2024) <https://www.cbn.gov.ng/Out/2024/RSD/Impact%20of%20Technology%20on%20Financial.pdf> accessed 23 September 2025

¹⁴ Ibid.

handle sensitive customer financial and personal data, thereby giving rise to various concerns pertaining to privacy¹⁵.

Nigeria possesses a well-developed financial system and digital infrastructure, which is expected to foster further advancements in sophisticated financial services¹⁶. These advancements may encompass business-to-business (B2B) liquidity and regulatory technology, specifically targeting anti-money laundering measures and know-your-customer (KYC) compliance¹⁷. Fintech companies in Nigeria are experiencing significant growth and success in various sectors, particularly in the domains of payment systems, distribution networks, and digital wallets¹⁸.

Therefore, it is imperative to ensure the safeguarding of consumer data against potential breaches and associated risks. Previously, the management of data was relatively uncomplicated, as it involved the utilisation of spreadsheets, tangible storage devices that are tangible, securable, and capable of being rendered nonfunctional when the data they contain becomes obsolete¹⁹. In the present era, owing to technological advancements and novel developments, the utilisation of data has become significantly sophisticated²⁰. For instance, contemporary smart phones possess the capability to capture and transmit location data, while automobiles are equipped with tracking systems. Moreover, real-time data processing has greatly facilitated the process of monitoring user activities in web and mobile applications, enabling the extraction of valuable insights through data mining techniques. The exposure of consumers to significant risks necessitates the implementation of appropriate regulations to effectively address these privacy concerns²¹.

¹⁵ Forester D, Guidorizzi M and Gabale S, 'What Fintech Companies Need to Know about Key Federal Privacy Requirements' (www.orrick.com 27 July 2022) <<https://www.orrick.com/en/Insights/2022/07/What-Fintech-Companies-Need-to-Know-About-Key-Federal-Privacy-Requirements>> accessed 25 July 2024.

¹⁶ Hassan Bello, Digitalisation and Financial System Stability: What Role for Macroprudential Policies? (Research Paper, Central Bank of Nigeria 2024) <https://www.cbn.gov.ng/out/2024/rsd/digitalisation%20and%20financial%20system.pdf> accessed 23 September 2025.

¹⁷ Ibid.

¹⁸ Udo Uduak Udo and Jacob Augustine, 'Bridging the Gap: Exploring the Role of FinTech in Advancing Financial Inclusion in Nigeria' (2025) 13 World Academics Journal of Management 22

¹⁹ Oluwasola Oni, Abayomi Oluwaseun Japinye and Gilbert Deinde Ifarajimi, 'Regulating Fintech for Financial Stability in Nigeria: Balancing Cybersecurity Risks and Financial Inclusion' (2025) 4 African Journal of Economics and Business Research (2) 2025.

²⁰ Awa Vernyuy, 'Impact of Technological Advancements on Human Existence' (2024) 3 International Journal of Philosophy 54.

²¹ Taviti Naidu Gongada and others, 'Technological Innovation Driven by Big Data' in Advanced Bioinspiration Methods for Healthcare Standards, Policies, and Reform (IGI Global 2022)

Fintech companies are increasingly recognizing the importance of data privacy and data management, particularly in the context of fintech²². These companies collect and analyze vast amounts of personal and financial data, requiring strict regulation to ensure user security and consumer well-being²³. The data protection law is the key regulation that govern the collection, analysis, and use of personal data. These regulations grant individuals the right to inspect, update, or modify their data, while also ensuring the availability of data content and legal entitlement to access ownership²⁴. Fintech firms must adhere to these regulations to provide secure services and protect users, while also avoiding liquidity and reputational risks²⁵.

The necessity for data security across various platforms is growing due to the widespread integration of financial technology in all facets of financial operations²⁶. In order to ensure the protection and autonomy of consumers' sensitive personal data, it is imperative for FinTech companies to enhance and uphold consumer control. Additionally, it is imperative to prioritise the exploration and implementation of emerging technologies to ensure the preservation of stability within the Nigerian financial sector and the protection of consumer financial information²⁷. The utilisation of both private and public channels is of utmost importance in enhancing operational standards within the financial technology sector, as the regulatory framework has consistently fallen behind the rapid pace of innovation²⁸.

3.0 OVERVIEW OF THE NIGERIA LEGAL FRAMEWORK OF DATA PROTECTION

²² Samuel Ayanboye, Odeniyi OA and Efunboade AO, 'An Analysis of the Effects of Data Privacy Legislation on Financial Technology Firms' (Paper presented at the Faculty Seminar, Faculty of Information and Information Technology, Osun State College of Technology, Esa-Oke, May 2025)

²³ Ibid.

²⁴ Ibid.

²⁵ Hazdun N, 'Council Post: Fintech Regulation: Legal and Regulatory Aspects' (*Forbes* 20 July 2022) <<https://www.forbes.com/sites/forbestechcouncil/2022/07/20/fintech-regulation-legal-and-regulatory-aspects/?sh=3f2a6ee62e38>> accessed 25 July 2024.

²⁶ Oluwaseyi Olakunle Mokuolu, 'Achieving Data Privacy and Security in Fintech Cloud Computing Environments' (2024) 23 World Journal of Advanced Research and Reviews 251

²⁷ Ibid.

²⁸ Catinas D and others, 'Data Privacy, Security, and Regulation in Financial Technology' (*The Henry M. Jackson School of International Studies* 25 June 2019) <<https://jsis.washington.edu/news/data-privacy-security-and-regulation-in-financial-technology/>> accessed 26 July 2024.

The adoption of digitalisation in Nigeria has resulted in the integration of technology into various sectors, thereby raising concerns regarding the management of data protection, processing, and enforcement²⁹. There must be equilibrium between safeguarding consumers from potential risks while respecting the fundamental rights of both consumers and other individuals³⁰. This has resulted in multiple endeavors by regulators to enact data protection legislation aimed at supervising matters pertaining to data privacy within the nation. The NDPR was implemented as the initial data regulatory framework preceding the more comprehensive Data Protection Act, which was developed to align with the European Union Guideline for Data Protection Regulation³¹.

The NDPR (National Data Protection Regulation) and the Data Protection Act provide an overview of the data protection laws in the United Kingdom, covering aspects such as the extent of the legislation, definitions of key terms, principles governing the processing of data, and mechanisms for enforcing compliance with data security practices³².

The widespread availability of communication accessibility has transformed the world into a global village, allowing users to access content and register for accounts. However, this also exposes individuals to potential risks, such as unauthorized access and exploitation of personal data. Cyber threats such as hacking, fraudulent activities, identity theft, and the extraction and sale of information can pose significant risks. Despite the widespread availability of mobile devices and laptops, maintaining access to these platforms is crucial for maintaining a secure global village³³.

There has been a noticeable increase in the implementation of data protection regulations by various jurisdictions worldwide. These regulations aim to safeguard the rights of individuals with regards to their personal data. They achieve this by imposing higher standards for data

²⁹ Moses Blessing, 'The Role of Technology in Strengthening Data Protection in Nigeria' (ResearchGate, October 2024) https://www.researchgate.net/publication/385175948_The_Role_of_Technology_in_Strengthening_Data_Protection_in_Nigeria accessed 23 September 2025.

³⁰ Ibid.

³¹ Olumide Babalola, 'The EU GDPR and Nigeria's NDPR: A Comparative Analysis' (2021) 4 Journal of Data Protection & Privacy 372

³² Preamble, Nigeria Data Protection Act, 2023

³³ International Network of Privacy Law Professionals, 'A Brief History of Data Protection: How Did It All Start?' (1 June 2018) <https://inplp.com/latest-news/article/a-brief-history-of-data-protection-how-did-it-all-start/> accessed 1 May 2025

protection practises that businesses must adopt to safeguard the personal data of their users. Additionally, these regulations seek to enhance ethical standards across different sectors³⁴.

According to the NITDA Act³⁵ in Nigeria establishes guidelines for electronic data exchange, aiming to protect privacy rights, secure financial transactions, and mitigate data manipulation. The Act applies to individuals residing within or outside Nigeria, and the Regulations impose compliance obligations on both private and public entities regarding the collection, processing, and utilization of personal data. The salient provisions of the NDPR are as follows:

The collection of personal data from a data subject must adhere to legal requirements and ensure that the data collected is sufficient, precise, and upholds the dignity of the individual.

The acquisition of consent from the individual must have been obtained in a voluntary manner, without the utilization of fraudulent tactics, coercion, or undue influence, prior to the commencement of data collection.

For the collection of Personal Data to be considered lawful, it is imperative that the data subject is informed of the specific purpose for which their consent is being obtained. The individual whose data is being processed must also be duly notified regarding their entitlement to withdraw their consent at any given point in time. The entity responsible for data management is required to exhibit its privacy policy in a clear and prominent manner. The individual whose data is being processed must also be duly informed regarding their entitlement to revoke their consent at any given moment. The entity responsible for managing data must clearly and prominently present its privacy policy.

The data should be stored for the required duration upon collection, ensuring it is protected from potential risks such as theft, cyberattacks, viral attacks, unauthorized dissemination, any form of manipulation, as well as damage caused by rain, fire, or exposure to other natural elements.

The collected data should be securely stored for the necessary duration, safeguarding it against potential threats such as theft, cyberattacks, viral attacks, unauthorised dissemination,

³⁴ An Overview of the Legal Framework of Data Protection in Nigeria' (ALP NG & Co, 2023) <https://www.alp.company/resources/business-advisory/overview-legal-framework-data-protection-nigeria> accessed 1 May 2025.

³⁵ The National Information and Technology Development Agency.

manipulation, and damage from environmental factors like rain, fire, or other natural elements.

Private institutions are required to appoint a Data Processing Officer in order to ensure meticulous adherence to the stipulations outlined in the Nigerian Data Protection Regulation (NDPR).

The implementation of the Nigerian Data Protection Regulation (NDPR) has facilitated Nigeria's progress in enhancing the protection of its citizens' privacy rights. Nevertheless, it is imperative for government agencies to exert additional endeavors to raise awareness among institutions regarding the significance of safeguarding data and to guarantee sufficient training and reorientation for institutions involved in the collection and processing of personal data pertaining to data subjects. Furthermore, it is important to acknowledge that the legal consequences for violating an individual's privacy rights result in a monetary penalty imposed on the offending institution, without providing any direct means of redress for the affected individual. In the future, it is suggested that privacy policies implemented by institutions may incorporate the provision of a predetermined monetary amount as recompense or restitution for the unauthorized sale or dissemination of individuals' personal data. Despite the absence of provisions granting individuals a personal entitlement to seek remedies, individuals who feel wronged still have the option to pursue legal action through a civil lawsuit, specifically for cases involving the conversion of private property or breach of contract, particularly in relation to confidentiality.

The Act, known as the Nigerian Data Protection Act, 2023, was enacted after the signing of the Nigerian Data Protection Bill, 2023. The Act establishes a legal structure for the oversight of personal data in Nigeria, a responsibility previously held by the Nigerian Data Protection Regulations (NDPR) 2019 under the National Information Technology Development Agency (NITDA) Act.

The Act establishes the Nigeria Data Protection Commission (NDPC), which is responsible for enforcing regulations pertaining to the processing of personal and sensitive data.

The Act aims to achieve several objectives. These objectives encompass the protection of fundamental rights, freedoms, and interests of data subjects as guaranteed by the Constitution of the Federal Republic of Nigeria, 1999 (as amended). Additionally, the Act seeks to regulate the processing of personal data in a manner that is fair, lawful, and accountable. It

also aims to promote practices that enhance the security of data processing and the well-being of data subjects. Lastly, the Act establishes a regulatory commission tasked with overseeing data protection matters. Moreover, the legislation aims to safeguard the rights of individuals whose data is being processed and establish mechanisms for seeking redress and remedies in cases where these rights are violated.

The salient provisions of the Nigeria Data Protection Act are³⁶

A) Establishment of a Commission that displaces the Nigeria Data Protection Bureau, empowered to see to the affairs of the data protection practices in the country.

B) The processing of personal data³⁷

Data must be processed lawfully, with fairness and transparency.

Data must be collected for the purpose for which it is collected – Purpose Limitation.

Data Minimization

Personal data must be stored securely for the purpose for which it was collected with consent – Storage Limitation.

Personal data must be processed accurately and consistently.

Personal Data must be collected and treated with confidentiality while ensuring the integrity of the data being processed.

Data controllers and Data Processors must be accountable for the data privacy of the data subjects.

C) According to regulatory guidelines, it is required that organizations notify relevant authorities within a timeframe of seventy-two hours following the identification of a data security breach. Additionally, in cases where the breach is determined to be of high risk after

³⁶ LawPavilion, 'Safeguarding Privacy: A Descriptive Analysis of the Nigeria Data Protection Act, 2023' (LawPavilion Blog, 22 June 2023) <https://lawpavilion.com/blog/safeguarding-privacy-a-descriptive-analysis-of-the-nigeria-data-protection-act-2023/> accessed 6 September 2023.

³⁷ Section 24, of the Nigeria Data Protection Act, 2023.

conducting a Data Protection Impact Assessment (DPIA), Organizations must also inform the individuals whose data has been compromised.³⁸

D) According to the Act, in the context of cross-border data transfers, it is required that the recipient, whether functioning as a data processor or data controller, must adhere to data regulations that are deemed adequate and enforceable at a level comparable to the Nigeria Data Protection Act.³⁹

The principles of data processing, as delineated in the aforementioned Act, are likewise upheld as principles within the framework of the General Data Protection Regulation (GDPR).⁴⁰ The primary focus lies in ensuring transparency to individuals whose data is being collected, utilised, stored, and processed. The data that has been gathered should possess the qualities of being readily accessible, as well as being presented in a manner that is both clear and comprehensible. It is imperative that data subjects are adequately informed about the purposes for which their data is being collected. Additionally, data subjects have a legitimate interest in knowing the entities responsible for processing their personal data. Therefore, it is necessary for data controllers and processors to disclose their identity. The accuracy and relevance of the specific purpose for collecting, storing, and utilising data must align with the intended rationale. The principle of data minimization stipulates that data should be stored in its most essential form, with the determination of this threshold typically falling under the purview of a data controller.⁴¹

According to the General Data Protection Regulation (GDPR), it is imperative to promptly report a breach notification within a 72-hour timeframe if the data breach is expected to pose a potential risk to the rights and freedoms of individuals whose data is involved. Data subjects must also be promptly notified of the risk to which they have been exposed, without any unnecessary delay.

³⁸ Section 40, of the Nigeria Data Protection Act, 2023.

³⁹ Section 41, 42, 43 of the Nigeria Data Protection Act, 2023.

⁴⁰ Chapter 2, Article 5-11 of the GDPR -EU.

⁴¹ Engineering WTWA of R in S and, 'Data Protection: A New Regulation in the European Union' (2016) 5 <https://www.academia.edu/28752959/Data_Protection_A_new_Regulation_in_the_European_Union> accessed 8 September 2023.

4.0 CHALLENGES OF THE DATA PROTECTION REGULATIONS IN NIGERIA

Vague Requirements and Phases

One of the primary difficulties encountered in the implementation of the Nigerian Data Protection framework pertains to the utilization of imprecise and unclear terminologies. For example, the mention of a "data controller and data processor of significant importance" by the act prompts inquiries regarding the interactions between data subjects and individuals involved in data processing. What does the term "major importance" encompass when considering the measures taken by data controllers and processors?

The General Data Protection Regulation (GDPR) in the United Kingdom (UK) is impeded in terms of compliance due to the presence of ambiguous language. The inclusion of vague terms such as "undue delay" and "disproportionate efforts" necessitates the establishment of precise definitions to ensure clarity and facilitate adherence to the regulation. The concept of a "reasonable level of protection" lacks specificity and clarity.

Extraterritorial Barrier

In the contemporary era of globalization. The implementation of the data protection act varies across countries, potentially imposing constraints on the cross-border transfer of data.

Consent to data collection

According to data protection legislation, organizations are prohibited from utilizing and gathering personal data without obtaining explicit consent from the individual to whom the data pertains. However, our findings indicate that Websites and Applications require individuals to consent to data processing by selecting the option "yes" to access their customer's information. Conversely, choosing the option "no" may result in denying access to the App as well as access to the website, both of which could be perceived as unjust and forceful.

Inadequate data literacy sensitization on data protection.

Despite the existence of data protection laws in Nigeria, such as the Nigerian Data Protection Regulation (NDPR) and its accompanying implementation framework, which includes the recently enacted data protection act, there remains a substantial number of individuals who

lack awareness regarding data protection practices yet have entrusted their personal data to numerous organizations. The prevalence of data illiteracy is a cause for concern, as it is incongruous with the pervasive digital nature of our society and the inherent exposure to data-related vulnerabilities that individuals encounter. Certain government agencies demonstrate a lack of awareness regarding the rights of data subjects, despite their involvement in handling large datasets pertaining to numerous individuals. Data is an invaluable asset for any organization, necessitating a collective responsibility among individuals at all hierarchical levels to ensure the security of consumer and personal data. The absence of knowledge will impede the advancement of the country's economic situation.

Lack of Enforcement of the provisions of the Nigeria Protection Act

Furthermore, due to the inadequate implementation of regulations pertaining to data breaches, there is a scarcity of legal actions and judicial precedents, resulting in a lack of awareness among individuals regarding their data rights and subsequent deprivation of these rights.

Lack of Trained Data Protection Professionals

The roles and responsibilities of data protection professionals have been a topic of interest since the establishment of the Data Protection Commission. However, it is worth noting that the full impact of the act, which may involve the establishment of branches across various states of the federation, to bring data protection to the grassroots and promote data literacy, has not yet been fully realised by the citizens. The country in question lacks a substantial number of adequately trained Data Protection Officers (DPOs), in contrast to Western countries that have successfully implemented their own data protection legislation. In the United Kingdom, numerous businesses have established the position of Data Protection Officer (DPO) in accordance with the stipulations outlined in the General Data Protection Regulation (GDPR).⁴²

It is anticipated that now there should be a reorganization in both the private and public sectors to align with the data protection act. This reorganization should involve the designation of Data Protection Officers (DPOs) within each business entity to fulfil the role of ensuring compliance. Additionally, there should be the establishment of a monitoring and supervisory authority that acts as an intermediary between internal and external stakeholders as well as regulatory bodies.

⁴² Article 37 of the GDPR EU.

GDPR is relevant to businesses as it mandates the use of automated processing for decision-making. Businesses must prioritize data security to ensure compliance with relevant legislation. If individuals' express objections to automated processing, businesses may need to focus on employee training and designating a Data Protection Officer⁴³.

6.0 Jurisdictional comparison

6.1 Appraisal of the Fintech Regulatory Framework in the United Kingdom

The United Kingdom has established itself as a global fintech leader by creating a regulatory environment that is both supportive of innovation and robust in its safeguards⁴⁴. At the heart of this success is a clear, growth-oriented philosophy championed by the government and enacted by agile regulators. Directives from the highest levels emphasize simplifying rules and reducing unnecessary burdens, shifting the focus toward outcomes rather than box-ticking compliance. This creates a climate where businesses can scale with confidence, knowing the regulatory framework is designed to facilitate, not hinder, their development⁴⁵.

A key feature of this approach is the proactive and hands-on role of the Financial Conduct Authority (FCA). The FCA operates a pioneering Regulatory Sandbox, allowing new companies to test innovative products in a controlled setting with real consumers, all under the regulator's guidance.⁴⁶ This de-risks the launch process for startups and provides the FCA with valuable insights into emerging technologies. Beyond the sandbox, the FCA's Innovation Hub and Advice Unit offer direct, tailored support to firms navigating complex rules. This "open-door" policy from the regulator is instrumental in building a collaborative ecosystem where innovation can thrive within clear guardrails.

The UK's regulatory structure itself is sophisticated yet clear. It operates under a "twin-peaks" model: the FCA focuses on protecting consumers, ensuring market integrity, and promoting competition, while the Prudential Regulation Authority (PRA) safeguards the

⁴³ Chika MDIYOKE, 'An Analysis of Data Protection and Compliance in Nigeria' (2020) IV <https://www.academia.edu/47771793/An_Analysis_of_Data_Protection_and_Compliance_in_Nigeria> accessed 11 September 2024.

⁴⁴ Preethi Vijayagopal, Bhawana Jain and Shyam Ayinippully Viswanathan, 'Regulations and Fintech: A Comparative Study of the Developed and Developing Countries' (2024) 17 Journal of Risk and Financial Management 324, 327.

⁴⁵ Ibid.

⁴⁶ Bryan Patrick, The Role of the Financial Conduct Authority (FCA) in Regulating FinTech in the UK (May 2025)

financial stability of major institutions⁴⁷. This division allows for expert oversight across different types of risk. The entire system is anchored by the Financial Services and Markets Act 2000 (FSMA), which sets the baseline for what activities require authorisation. The rules are deliberately technology-neutral, meaning core principles of fairness, transparency, and accountability apply whether a firm uses traditional methods or cutting-edge artificial intelligence, ensuring safety without prematurely stifling new ideas⁴⁸.

In addition, instead of rushing to impose sweeping bans or complex new laws, the UK has taken a measured, step-by-step approach. It began by clarifying how existing financial rules apply to different types of crypto tokens and brought crypto businesses under anti-money laundering supervision⁴⁹. It then strengthened consumer protection by applying strict marketing and risk-warning rules to crypto promotions. Now, the government is gradually introducing a broader regulatory regime for crypto activities, focusing on the specific services provided rather than creating panic with reactive legislation⁵⁰. This methodical progression manages immediate risks while building a credible long-term framework for the industry⁵¹.

Finally, the UK's strength lies in its deep support for specialization across the entire financial technology spectrum. It is a European powerhouse in WealthTech and was an early adopter of Open Banking, which it is now expanding into broader "Open Finance." The ecosystem actively nurtishes niches like RegTech, where technology streamlines compliance, and InsurTech, where firms can use regulatory tools like the Digital Sandbox to test products involving smart contracts and data analytics⁵². By providing these tailored pathways and tools, the UK ensures its fintech sector remains diverse, competitive, and at the forefront of global innovation.⁵³

6.2 Lessons for Nigeria Legal Framework

6.2.1 Adoption of Pro-Growth, "Open-Door" Regulatory Mindset

⁴⁷ Ibid.

⁴⁸ Ibid.

⁴⁹ 'Fintech Laws and Regulations 2025 – United Kingdom' (Global Legal Insights, 1 September 2025) <https://www.globallegalinsights.com/practice-areas/fintech-laws-and-regulations/united-kingdom/> accessed 23 September 2025

⁵⁰ Ibid.

⁵¹ Ibid.

⁵² Giovanni Cornelli, Sebastian Doerr, Leonardo Gambacorta and Ouarda Merrouche, 'Regulatory Sandboxes and Fintech Funding: Evidence from the UK' (forthcoming) Review of Finance

⁵³ Ibid.

Nigeria's regulators must transition from a purely enforcement-based posture to one that actively partners with innovators. Emulating the UK's Financial Conduct Authority (FCA), the Central Bank of Nigeria (CBN) and Securities and Exchange Commission (SEC) should establish a dedicated, empowered Fintech Innovation Office. This office would not just make rules but would provide direct, tailored guidance to startups, demystifying compliance and de-risking innovation. A clear, publicly communicated policy prioritizing market growth alongside consumer protection is essential to attract and retain investment.

6.2.2 Ensure Rules are Technology-Neutral and Principles-Based

Nigeria's new regulations, including the Data Protection Act, should avoid being overly prescriptive about specific technologies. Instead, they should establish strong, outcome-based principles (e.g., "treat customers fairly," "ensure data security," "maintain market integrity") that apply equally to a traditional bank and a blockchain-based fintech. This future-proofs the regulatory framework, allowing innovation to flourish within a stable and understandable set of core obligations, mirroring the durability of the UK's FSMA.

Take a Phased, Activity-Based Approach to Crypto and Emerging Tech

Rather than reactive bans or overly complex, premature legislation, Nigeria should follow the UK's phased, risk-based methodology. The immediate priority should be bringing all crypto asset service providers under robust Anti-Money Laundering (AML) and consumer promotion rules to tackle fraud and protect investors. Subsequently, a clear, consultative roadmap should be published for the gradual introduction of a broader regulatory framework, focusing on regulating specific activities (like trading, custody, and issuance) rather than attempting to define every type of digital asset in a fast-moving market.

7.0 CONCLUSION AND RECOMMENDATION

The Nigeria Data Protection Act, as the recent primary legislation, represents a significant and commendable endeavor aimed at fostering the adoption of data protection measures within the technology sector and other pertinent industries in Nigeria. Nigeria has made progress by initiating measures to implement the legislative and judicial provisions of the Act. This implementation is crucial in establishing a significant and favorable disparity between the previous data protection laws and the Act. It signifies the country's commitment

to effectively manage data governance in a distinct manner. Regulators must exhibit a strong commitment to enforcing the provisions of the Act.

Despite the commendable provisions, the Act exhibits certain deficiencies, namely the perceived absence of independence of the commission established under the Act, lack of clarity regarding its applicability to artificial entities, and the absence of a specified timeline for responding to data subject access requests (DSARs). To elevate our Act to a globally recognized standard, it is imperative to undertake a comprehensive revision aimed at rectifying the existing loopholes.