International Journal of Innovative Information Systems & Technology Research 13(4):304-312, Oct-Dec, 2025

© SEAHI PUBLICATIONS, 2025 www.seahipublications.org ISSN: 2467-8562

doi:10.5281/zenodo.17774262

Assessment Of National Data Protection Regulation In The Financial Industry

***Suleiman Muhammad-Kabir Abdullahi; Prof. U. M. Mbanaso; Dr. M. O. Adenomon & Dr. S. E. Chaku**

Centre for Cyberspace Studies,
Nasarawa State University Keffi, Nigeria

***muhammadkabirsuleiman6@gmail.com**

ABSTRACT

The increasing digitization of the financial industry has elevated the importance of robust data protection mechanisms to safeguard sensitive customer information. This study critically assesses national and international data protection regulations, focusing on their impact on the financial sector, with particular reference to the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) and Nigeria Data Protection Regulation. It explores the compliance challenges financial institutions face, especially in the context of emerging technologies such as artificial intelligence, blockchain, and big data analytics. Employing a qualitative research design, the study gathers insights from regulatory experts, data protection officers, and legal advisors using purposive sampling and thematic analysis. The findings highlight inconsistencies in global data protection standards, rising compliance costs, and a growing need for a harmonized, adaptive regulatory framework. The research emphasizes the role of Regulatory Technology (RegTech) and institutional culture in ensuring effective compliance. Ultimately, this study contributes to policy discourse by proposing strategic frameworks that can enhance data protection, reinforce consumer trust, and improve institutional resilience in the face of evolving cyberthreats.

Keywords: Data Protection, GDRP, CCPA, Financial Instituttion, Regulatory Conpliance, RegTech, Cybersecurity, Consumer Trust, Nigeria Delta Protection Regulation, Nigeria Central Bank

INTRODUCTION

The financial industry has witnessed a dramatic transformation in recent decades, driven by rapid technological advancements and the extensive digitization of services. While this digital revolution has enhanced operational efficiency, convenience, and customer experiences, it has simultaneously introduced profound risks regarding data security and privacy (Terry, 2018). As financial institutions collect, store, and process vast quantities of sensitive personal data, the imperative for robust data protection has become paramount.

The vulnerability of financial data is underscored by the growing incidence of cyberattacks and high-profile data breaches, such as the 2017 Equifax incident. These events have catalyzed a global regulatory response, most notably the implementation of the General Data Protection Regulation (GDPR) by the European Union and the California Consumer Privacy Act (CCPA) in the United States. These

frameworks have set global benchmarks, inspiring similar legislative efforts like the Nigeria Data Protection Regulation (NDPR) (Van Duyne, 2020; Rich, 2020).

However, the rapid digitalization of the sector has outpaced these regulatory frameworks. Financial institutions now face the dual challenge of navigating a fragmented and complex regulatory landscape while defending against sophisticated cyber threats. The lack of comprehensive global standards has resulted in inconsistent protection levels and "patchwork" compliance strategies that drive up operational costs (Moromoke et al., 2024). Furthermore, emerging technologies such as artificial intelligence, blockchain, and big data analytics often exploit gaps in current legislation, posing new security risks.

This study addresses these critical issues by assessing national data protection regulations—specifically focusing on the NDPR alongside international benchmarks like GDPR. It seeks to understand the friction between regulatory compliance and operational efficiency, aiming to contribute to the development of a harmonized, adaptive regulatory framework that ensures the safeguarding of sensitive financial data (Al-Omiri et al., 2017; Ruiu et al., 2021).

Research Questions

Based on the identified problems and the scope of the study, the following research questions will guide the investigation:

RQ1: How do key data protection regulations (such as GDPR, CCPA, and NDPR) impact the compliance efforts and operational costs of financial institutions?

RQ2: What are the specific challenges financial institutions face when implementing data protection measures amidst emerging technologies like AI and blockchain?

RQ3: To what extent does the current fragmentation of global data protection standards affect consumer trust and data security?

RQ4: What are the essential components required to establish a harmonized and adaptive regulatory framework for the global financial industry?

Research Objectives

The primary aim of this study is to assess national data protection regulations within the financial industry. To achieve this, the specific objectives are:

- To Analyze the key data protection regulations (GDPR, CCPA, NDPR) and evaluate their impact on financial institutions' operational and compliance landscapes.
- To Assess the challenges and identify best practices associated with regulatory compliance, particularly regarding the integration of emerging technologies (AI, Blockchain, Big Data).
- To Propose a harmonized and adaptive regulatory framework that bridges the gap between technological advancement and legal enforcement to ensure consistent cross-border data protection.

Hypothesis 1 (Impact on Operations):

H 0 : The implementation of diverse data protection regulations (GDPR, NDPR) has no significant relationship with the increase in operational costs for financial institutions.

H 1 : The fragmentation and complexity of current data protection regulations are significantly correlated with increased operational costs and compliance burdens for financial institutions.

Hypothesis 2 (Technology vs. Regulation):

H 0 : Existing regulatory frameworks are sufficient to mitigate data security risks introduced by emerging technologies (AI, Blockchain).

H 1 : Current regulatory frameworks possess significant gaps that fail to adequately mitigate security risks introduced by emerging technologies, necessitating an adaptive regulatory approach.

Hypothesis 3 (Harmonization and Trust):

H 0 : A harmonized global regulatory framework will not significantly affect consumer trust in financial institutions.

H 1 : The adoption of a harmonized and adaptive regulatory framework is positively correlated with enhanced consumer trust and improved data security posture in the financial sector.

Literature Review

Albrecht et al. (2019) analyzed European financial institutions post-GDPR and found that while basic measures were in place, the depth of compliance varied significantly due to the complexity of the regulations. Voigt and Von dem Bussche (2017) noted that institutions with centralized data governance frameworks achieved higher compliance levels than those with fragmented legacy systems. In the context of the CCPA, Tankard (2020) highlighted a gap in consumer awareness, suggesting that while regulations exist, their effectiveness relies heavily on public education and institutional transparency.

The integration of advanced technologies presents a double-edged sword. Wirth (2018) and Chen et al. (2021) found that while AI enhances analytical efficiency, it introduces algorithmic bias and new cybersecurity vulnerabilities. Similarly, Wang et al. (2019) and Finck (2019) identified a critical tension between Blockchain technology and data protection laws. Specifically, the immutability of blockchain records conflicts with the GDPR's "right to be forgotten," creating a legal-technical paradox that requires urgent regulatory resolution.

A recurring theme in recent literature is the challenge of regulatory fragmentation. Greenleaf (2019) and Schwartz and Peifer (2017) argue that the divergence between different national frameworks (e.g., the US sectoral approach vs. the EU comprehensive model) creates substantial friction for multinational institutions. These discrepancies increase compliance costs and necessitate a "patchwork" approach to data security. Consequently, there is a strong consensus in the literature advocating for harmonized international standards to facilitate cross-border data flows and ensure consistent global protection.

METHODOLOGY

This study adopts a qualitative research design rooted in the interpretivism paradigm, which seeks an in-depth understanding of the subjective experiences and practical complexities of data protection in the Nigerian financial sector (Kothari, 2004). The design allows for the exploration of attitudes, perceptions, and implementation challenges faced by key regulatory and institutional actors in aligning local standards, particularly the NDPR, with global benchmarks like the GDPR. The target population comprises senior executives and data protection officers at the Central Bank of Nigeria (CBN) and major Nigerian banks, as well as relevant legal and regulatory experts.

Data will be collected using purposive sampling to ensure the selection of highly knowledgeable participants, with the questionnaire serving as the primary instrument for gathering rich qualitative data. This method allows for anonymity and the systematic collection of insights across various themes, including the CBN's compliance approach, the impact of emerging technologies (AI/Blockchain), and the influence of local regulations. The collected data will be subjected to rigorous thematic analysis to identify recurring patterns related to institutional capacity and regulatory challenges, complemented by content analysis of regulatory documents. While the study is qualitative, a simplified conceptual model is used to frame the relationships between Regulatory Compliance (RC) and factors like Technological Adoption and Institutional Capacity (RC=f(TA,IC,SE,EC)), providing a structured basis for interpreting the qualitative findings through tools like SWOT and Force Field Analysis.

RESULTS AND DISCUSSION

Table 1: Awareness and Compliance with Data Protection Regulations (n = 20)

Statement	SA	A	N	D	SD
CBN staff are aware of data protection policies	25%	45%	15%	10%	5%
Banks have sufficient awareness of NDPR requirements	20%	40%	20%	15%	5%
Compliance training is regularly conducted	10%	35%	25%	20%	10%
Data protection is prioritized in financial operations	15%	40%	20%	15%	10%

Overall, 70% of respondents agreed or strongly agreed that data protection awareness exists within CBN and banks, though 25% were neutral or disagreed. This indicates fair awareness but inconsistent enforcement.

As one CBN respondent noted, "Although the NDPR provides a good framework, enforcement at the operational level is weak due to lack of monitoring resources."

Table 2: Technological Adoption and RegTech Implementation (n = 20)

Statement	SA	A	N	D	SD
Our institution uses AI or RegTech tools for compliance	15%	25%	25%	20%	15%
CBN encourages the use of emerging technologies	20%	35%	25%	15%	5%
Technological infrastructure supports full data compliance	10%	30%	20%	25%	15%
Cost of technology limits implementation	30%	45%	10%	10%	5%

55% agreed that technological tools are being adopted, though 45% indicated slow or limited use due to infrastructure and cost barriers.

A DPO respondent remarked, "Our bank has implemented AI for customer verification, but legacy systems slow down full compliance automation."

Table 3: Institutional Capacity and Human Capital Readiness (n = 20)

Statement	SA	A	N	D	SD
Our institution has a dedicated compliance unit	20%	25%	15%	25%	15%
Staff are trained regularly on data protection	10%	30%	25%	20%	15%
External consultants are relied upon for audits	35%	40%	15%	5%	5%
Human resource capacity is sufficient for compliance	10%	25%	25%	25%	15%

45% agreed that institutional structures exist for compliance, while 50% admitted overreliance on external consultants.

One respondent noted, "We rely on external consultants for audits because we don't have a dedicated compliance unit."

Table 4.4: Consumer Trust and Public Perception (n = 20)

Statement	SA	A	N	D	SD
Customers trust banks to protect personal data	20%	35%	25%	15%	5%
Public awareness of data rights is improving	15%	40%	20%	15%	10%
Data transparency improves institutional reputation	25%	45%	20%	5%	5%
Breaches negatively affect public confidence	40%	45%	10%	5%	0%

While 75% agreed that transparency improves reputation, only 55% believe public awareness is strong. Most respondents emphasized that customer trust depends on consistent data handling.

A legal advisor stated, "Customers are starting to ask questions about their data rights, especially after hearing about breaches in the news."

Table 4.5: Regulatory Challenges and Fragmentation (n = 20)

Statement	SA	A	N	D	SD
Local regulations align with international data standards	15%	30%	25%	20%	10%
Conflicts exist between NDPR and global laws (e.g., GDPR)	35%	45%	10%	5%	5%
CBN policies provide sufficient regulatory clarity	20%	35%	20%	15%	10%
Lack of coordination hinders cross-border compliance	30%	40%	15%	10%	5%

A combined 70% agreed that inconsistencies between local and global laws create compliance confusion. One expert summarized, "The lack of alignment between CBN policies and international data privacy laws creates confusion during cross-border transactions."

Table 6: Summary of Findings Across Themes (n = 20)

Theme	Dominant Response	% Agreement (SA + A)	Key Observation
Awareness & Compliance	Moderate	70%	Awareness present, enforcement weak
Technological Adoption	Low-Moderate	55%	Adoption slow due to cost & infrastructure
Insitutional Capacity	Weak	45%	Reliance on external consultants
Consumer Trust	Moderate	65%	Awareness improving, still limited
Regulatory Challenges	High Concern	75%	Conflicts between local and global laws

The results reveal that while CBN and related institutions show progress in awareness and partial compliance, challenges persist in technology adoption, institutional readiness, and legal harmonization.

Quantitatively, average agreement across all areas was 62%, showing moderate engagement but structural limitations in full data protection compliance.

These findings align with prior literature (Albrecht et al., 2019; Greenleaf, 2019; Masrom & Ismail, 2020), emphasizing the need for stronger institutional frameworks, regulatory coherence, and increased public education on data privacy.

DISCUSSION OF FINDINGS

The analysis of data from 20 respondents provides a balanced perspective on the current state of data protection compliance in Nigeria's financial sector. The results confirm that while awareness of the NDPR and related global frameworks is growing, there are still notable gaps in technological adoption, institutional capacity, and regulatory clarity.

From the findings, 70% of respondents acknowledged strong awareness of data protection policies, confirming that CBN-led sensitization efforts are effective. However, compliance implementation remains weak due to limited monitoring and uneven institutional readiness. This supports Regulatory Compliance Theory (Parker & Nielsen, 2011), which posits that organizations often comply out of obligation rather than embedded culture.

Regarding technology adoption, only 55% of respondents agreed that their institutions use RegTech or AI tools for compliance, while nearly half noted that high costs and outdated infrastructure hinder progress. This pattern aligns with Innovation Diffusion Theory (Rogers, 2003), suggesting that the rate of adopting new technologies depends on perceived compatibility and ease of integration. Nigerian financial institutions, though aware of the benefits, remain constrained by resources.

Institutional capacity findings show that 50% of respondents rely heavily on external consultants due to insufficient internal expertise. This supports Institutional Theory (DiMaggio & Powell, 1983), where compliance is often symbolic—meant to project legitimacy rather than establish deep-rooted operational change. The lack of specialized compliance units limits sustainable enforcement.

In terms of consumer trust, 65% of respondents believe that transparent data practices improve institutional reputation, though public awareness remains low. This reinforces the findings of Martin & Murphy (2020), who linked consumer confidence to open communication about data usage. The Nigerian context, however, still lacks adequate education and awareness initiatives to fully engage customers.

Lastly, 75% of respondents identified inconsistencies between local and global data protection laws as a major barrier to effective compliance. This echoes Schwartz & Peifer (2017) and Greenleaf (2019), who

both emphasized the need for harmonized data frameworks to support international data transfers. The Nigerian case reflects a growing recognition of this need, especially as the financial sector becomes increasingly digital and globally connected.

Overall, the findings support the combined theoretical model, demonstrating that regulatory compliance is influenced by technological capacity, institutional readiness, stakeholder engagement, and external policy alignment. While Nigeria's financial sector is moving in the right direction, it still requires greater institutional investment and inter-agency coordination to achieve full regulatory maturity.

CONCLUSION

This study concludes that the Central Bank of Nigeria plays a pivotal role in shaping data protection and compliance practices within the financial sector. However, the level of compliance across institutions is still below optimal standards. The findings confirm that awareness alone is not sufficient — effective compliance requires robust institutional structures, skilled personnel, and a strong culture of accountability.

The research validates Regulatory Compliance Theory, showing that enforcement mechanisms and institutional alignment significantly influence compliance outcomes. It also supports Innovation Diffusion Theory, indicating that adoption of new technologies like RegTech depends on awareness, perceived benefits, and financial capacity.

While progress has been made since the introduction of the NDPR, Nigeria's data protection landscape remains in transition. Achieving full compliance

RECOMMENDATIONS

Based on the study findings, the following recommendations are proposed to strengthen data protection and regulatory compliance within Nigeria's financial system:

- Strengthen Enforcement Mechanisms

The CBN and National Data Protection Commission (NDPC) should enhance enforcement of existing data protection laws through regular audits, monitoring, and sanctions for non-compliance.

- Capacity Building and Training

Financial institutions should invest in continuous training programs for compliance officers, IT staff, and senior management to develop in-house expertise in data governance.

- Adoption of RegTech Solutions

The CBN should promote the integration of RegTech and other digital compliance tools to automate monitoring, reporting, and risk detection, reducing manual errors and improving efficiency.

- Public Awareness and Consumer Education

Awareness campaigns should be launched to educate consumers about their data protection rights and how to identify misuse of their personal data.

- Policy Harmonization

The NDPR should be aligned more closely with international frameworks such as the GDPR to facilitate cross-border data exchange and improve investor confidence.

- Incentives for Compliance

Institutions that demonstrate strong compliance behavior should be publicly recognized or granted regulatory incentives to encourage wider adoption across the sector.

- Collaboration Among Stakeholders

Strengthening collaboration between the CBN, NDPC, and financial service providers will ensure uniform implementation of standards and reduce policy conflicts.

REFERENCES

Albrecht, J. P., Dean, T. J., &Brodbeck, A. (2019). GDPR compliance and the financial sector: An empirical analysis. Journal of Financial Regulation, 5(2), 234-259.

Barney, J. (1991). Firm Resources and Sustained Competitive Advantage. Journal of Management, 17(1), 99-120.

Becker, G. S. (1968). Crime and Punishment: An Economic Approach. Journal of Political Economy, 76(2), 169-217.

California Consumer Privacy Act (CCPA). (2020). Retrieved from https://oag.ca.gov/privacy/ccpa

California Legislative Information. (2020). California Consumer Privacy Act (CCPA).

California Legislative Information. (2020). California Consumer Privacy Act (CCPA).

Casino, F., Dasaklis, T. K., &Patsakis, C. (2019). A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification, and Open Issues. Telematics and Informatics, 36, 55-81.

Casino, F., Dasaklis, T. K., &Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification, and open issues. Telematics and Informatics, 36, 55-81.

Chen, J., Zhang, C., & Xu, Y. (2021). AI adoption in financial services: Implications for data privacy and ethics. *Journal of Financial Innovation*, 7(3), 112–128.

Compliance Challenges and Best Practices:

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319-340.

Deloitte. (2020). Navigating the complexities of data privacy regulations: Best practices for financial institutions. Retrieved from https://www2.deloitte.com/global/en/pages/ risk/articles/navigating-complexities-of-data-privacy-regulations.html

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. American Sociological Review, 48(2), 147-160.

Ernst & Young (EY). (2018). Data protection and privacy regulations: How financial institutions are navigating compliance challenges. Retrieved from https://www.ey.com/en_gl/financial-services/data-protection-privacy-regulations

Finck, M. (2019). Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law? *European Parliamentary Research Service*.

Gai K, Qiu M, Sun X. A survey on fintech. Journal of Network and Computer Applications. 2018;103:262-273. doi:10.1016/j.jnca.2017.10.011.

Global Standards for Data Protection:

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact. International Journal of Market Research, 59(6), 703-705.

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. International Journal of Market Research, 59(6), 703-705.

Greenleaf, G. (2012). Global Data Privacy Laws: 89 Countries, and Accelerating. Privacy Laws & Business International Report, 115, 11-17.

Greenleaf, G. (2014). Asian data privacy laws: Trade and human rights perspectives. Oxford University Press.

Greenleaf, G. (2019). Global data privacy laws: 100 countries, and accelerating. Privacy Laws & Business International Report, 157, 11-17.

Hopkin, P. (2018). Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management. Kogan Page Publishers.

Hossain, M. I., & Karim, M. (2021). Information governance and regulatory compliance in financial institutions: A structural approach. *International Journal of Information Management*, 56, 102262.

Hughes-Lartey, S. (2019). Data Protection Compliance Challenges in the Financial Industry. Journal of Financial Regulation and Compliance, 27(3), 310-329.

Hughes-Lartey, S. (2019). Data protection compliance challenges in the financial industry. Journal of Financial Regulation and Compliance, 27(3), 310-329.

Kamarinou, D., Millard, C., & Singh, J. (2016). Machine Learning with Personal Data. Queen Mary School of Law Legal Studies Research Paper No. 247.

Kamarinou, D., Millard, C., & Singh, J. (2016). Machine learning with personal data. Queen Mary School of Law Legal Studies Research Paper No. 247.

Kshetri, N. (2014). Big data's impact on privacy, security and consumer welfare. Telecommunications Policy, 38(11), 1134-1145.

Martin, K., & Murphy, P. (2020). The role of transparency in building consumer trust in financial institutions. *Business Ethics Quarterly*, 30(2), 173–199.

Masrom, M., & Ismail, N. (2020). Organizational readiness and data protection compliance: A study of the Malaysian financial sector. *Asian Journal of Business and Accounting*, 13(1), 145–167.

Parker, C., & Nielsen, V. L. (2009). Compliance: A scholarly enterprise? In Parker, C. & Nielsen, V. L. (Eds.), Explaining Compliance: Business Responses to Regulation. Edward Elgar Publishing.

Radanliev, P., De Roure, D., Nurse, J. R., Montalvo, R. M., Nicholls, R., Cannady, S., &Burnap, P. (2020). Cyber risk at the edge: Current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains. Cyber-Physical Systems, 6(1), 1-22.

Rich J. CCPA and its impact on financial services. The Banking Law Journal. 2020;137(1):30-39.

Rogers, E. M. (1962). Diffusion of Innovations. Free Press.

Schwartz, P. M. (2019). Global data privacy: The EU way. New York University Law Review, 94, 771-818.

Schwartz, P. M., & Peifer, K. N. (2017). Transatlantic data privacy law. *Georgetown Law Journal*, 106(1), 115–178.

Tankard, C. (2020). What the CCPA means for business. Network Security, 2020(1), 8-10.

Technological Advancements and Data Security Risks:

Terry M. Cross-border data sharing under GDPR: Implications for financial institutions. Data Privacy Review. 2018;12(5):45-60.

Van Duyne PC. Money laundering policy: Fears and facts. Criminal Law Forum. 2020;13(1):311-328.

Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer.

Voigt, P., & Von demBussche, A. (2017

Voigt, P., & von demBussche, A. (2017). The EU General Data Protection Regulation (GDPR). Springer International Publishing.

Voigt, P., & Von demBussche, A. (2017). The EU General Data Protection Regulation (GDPR). A Practical Guide. Springer.

Zhang, B., & Dafoe, A. (2019). Artificial Intelligence: The Societal Impact of Emerging Technologies. Daedalus, 148(2), 25-42.