PERCEPTIONS OF DATA PROTECTION COMPLIANCE AMONG SOFTWARE ENGINEERS IN NIGERIA FINANCIAL TECH

Chika Michael Diyoke
RETRIDOL, National Open University of Nigeria
&
Onyekachi Obute
.NET Backend Developer Stanbic IBTC Bank

Abstract
Data protection compliance has emerged as a central issue in Nigeria's growing financial technology (FinTech) ecosystem, where vast amounts of sensitive personal data are processed daily. However, concerns remain regarding how well software engineers who create and manage FinTech systems understand and implement regulatory frameworks such as the Nigerian Data Protection Regulation (NDPR) and the European Union's General Data Protection Regulation (GDPR). The study therefore, examined the perceptions of data protection compliance among software engineers in Nigerian FinTech companies. Specifically, the objectives of the study were to examine the level of familiarity of software engineers in Nigerian FinTech companies with data protection laws; assess how software engineers perceive their role in protecting user data and the extent to which they implement data protection practices; and identify the challenges software engineers face in complying with data protection regulations. The study adopted a mixed-methods design comprising a quantitative survey of 113 engineers and qualitative Key Informant Interviews with compliance managers across leading Lagos-based FinTech firms. The analysis revealed a significant positive correlation between awareness of data protection laws and responsible compliance behaviour ($r = .582$, $p < .01$). However, practical compliance remains constrained by inadequate training, limited managerial support, and the absence of localized compliance tools. The study concludes that awareness alone is insufficient to ensure compliance unless it is supported by strong institutional frameworks and the integration of privacy-by-design principles into software development processes. It recommends, among other measures, the provision of hands-on data protection training for engineers, the integration of privacy considerations into all stages of software development, and investment in modern security tools

Keywords: Data Protection, Fintech, Software Engineers, Nigeria Data Protection Regulation (NDPR), Compliance

Background to the Study

Over the last few years, Companies like Paystack and PiggyVest are at the forefront of Nigeria's fintech revolution. Paystack, for example, drives over 60,000 companies across Nigeria and Ghana, like FedEx, UPS, and MTN, via secure online payment systems (TechCrunch, 2020). PiggyVest, on the other hand, has transformed traditional saving methods by digitizing the local *kolo* (piggy bank), and Nigeria's digital economy has undergone a period of tremendous transformation. The contribution of financial technology (fintech) cannot be overstated. Mobile payment systems, digital credit facilities, and mobile banking applications have all developed as major support systems for Nigeria's economic growth. This surge is driven by a youthful population, mobile phone penetration, and the urgency to close the financial inclusion gap (CBN, 2020). users to automate their savings and achieve financial goals more easily (Mordi, 2021). Nigeria's financial inclusion has improved significantly because of such advances. By 2023, 64% of Nigerians had access to formal financial services, up from 56% in 2020, thanks primarily to digital technologies such as agent banking and mobile money platforms (EFInA, 2023). But with more financial services online, the stakes and visibility of personal information have grown. That information isn't just used to tailor advertising or improve service; it also plays a critical role in detecting deception and fueling machine decisions. Despite anonymization technologies, including encryption, pseudonymization, and data masking being commonly utilized to protect individuals from revealing their identities, studies have shown that anonymized data can be traced in some instances, bringing the individual to the attention of profiling, discrimination, or exploitation for financial reward (Ohm, 2010; McMillan LLP, 2024).

Globally, cyberattacks and breaches continue to highlight the importance of increased cybersecurity in the financial industry. A recent example was in 2024, when LockBit 3.0 organized a large-scale ransomware attack on America's banking-as-a-service company Evolve Bank & Trust. Private customer information, including account numbers and deposit data, was stolen and dumped on the dark web. Fintech firms such as Wise and Mercury, which collaborate with Evolve, discovered that their customers were harmed, demonstrating how

sophisticated systems can be exposed when technology defenses are compromised (Cyber Management Alliance, 2024).

In Nigeria here, the fintech sector is also faced with increasing cybersecurity attacks that could jeopardize its growth. In 2022 alone, the Nigerian Communications Commission documented over 150,000 phishing attacks on the banking and financial sectors, representing increasing levels of sophistication among cyberattacks. This is a telling experience that even with advanced infrastructure, these organizations can be targeted by cyber-attacks, and this underscores the imperative need for strong data governance and proactive security measures in the fintech sector.

In response to increasing data privacy dangers, countries have come up with a range of legislation safeguarding how personal data are handled. Among the most impactful of these is the General Data Protection Regulation (GDPR) of the European Union, which was passed in May of 2018. The GDPR transformed privacy law, with a great deal of focus being placed upon such notions as data minimization, user consent, right to be forgotten, and levying severe fines on recalcitrant companies (Fausto, 2018). Frameworks like the EU-US Privacy Shield also attempt to control how US companies handle European citizens' data in transboundary settings.

In Nigeria, the National Information Technology Development Agency (NITDA) did the same, in line with its 2007 Act, by issuing the Nigeria Data Protection Regulation (NDPR) in January 2019. NDPR, though inspired by GDPR, was nevertheless carefully adapted to Nigeria's own economic and social conditions in crafting not just a legal framework but a pioneering institutional move to protect personal data.

Although these guidelines exist, it is often up to software developers to put them into action, particularly in fast-growing areas such as finance. These technology specialists design and manage the internet-based platforms through which personal information travels every day. Unfortunately, research reveals a significant gap: engineers frequently lack the necessary knowledge or tools to transform compliance requirements into safe, compliant systems (Diyoke & Edeh, 2020; Franke et al., 2024; Sabo & Utulu, 2023). This study, therefore, explores the degree at which Nigerian fintech software developers understand, perceive, and apply data protection rules, with the goal of evaluating gaps and giving recommendations on how to enhance compliance.

Statement of Problem

While the fintech sector in Nigeria has seen significant growth (CBN, 2020; EFInA, 2023), the concern over data privacy and protection is becoming more necessary. Whilst there have been regulatory frameworks like the Nigeria Data Protection Regulation (NDPR) to ensure the secure processing of personal data (NITDA, 2019), it is the duty of software developers to enforce such measures. Nonetheless, there is mounting evidence of a vast disparity between what is demanded by the rules and what takes place (Diyoke & Edeh, 2020; Franke et al., 2024). Again, many software developers are not properly trained, equipped, and guided on how to map legal requirements into secure and compliant systems (Sabo & Utulu, 2023). A good example is a situation where a fintech company can obtain a privacy policy that checks all the boxes for NDPR compliance but contains loopholes, such as failing to encrypt customers' data or protecting its APIs that leave the system vulnerable to cyber-attacks. The 2024 cyberattack on Evolve Bank & Trust, which also affected big fintech names like Wise and Mercury, is a good example of how exposed systems (ComplexDiscovery, 2024). Despite the cutting-edge infrastructures of these businesses, the attack still led to sensitive financial data being leaked on the dark web.

This expanding gap not only exposes fintech firms to prospective penalty or reputational damage but also puts at risk millions of customers with critical exposure to invasions, profiling, discrimination, and even financial abuse (Ohm, 2010; McMillan LLP, 2024). Considering this, understanding how software engineers perceive, handle, and react to data protection legislation is more important than ever. If Nigeria's digital economy is to continue developing in safety, such findings could have an influential role to play in creating stronger, safer foundations right from the start.

Research Questions

The following research questions guided this study:

1. How familiar are software engineers in Nigerian fintech companies with data protection laws like NDPR and GDPR?
2. How do software engineers view their role in protecting user data, and how do they put this into practice?
3. What challenges do engineers face when trying to follow data protection rules, and what can help make compliance easier?

Research Hypotheses

1. There is no significant relationship between software engineers' awareness of data protection regulations and their ability to implement compliance measures.
2. Access to training and technical resources does not significantly reduce the challenges software engineers face in complying with data protection regulations.

Review of Related Literature

Studies across literature in both developing and developed countries all demonstrate a knowledge gap among technical staff of data protection law. For instance, in a nearby study by Sabo and Utulu (2023) with the title "Organization Studies Based Appraisal of Institutional Propositions in the Nigeria Data Protection Regulation," the authors ascertained the degree of knowledge and awareness of the Nigeria Data Protection Regulation (NDPR) among fintech companies, technical departments, and software developers. Using a qualitative approach that involved interviewing and institutional analysis, they concluded that while fintech firms had some company-level understanding of the NDPR, virtually no training was given to software engineers in terms of interpreting or applying the regulation in their operations. The study highlighted the existence of a gap between governance-level compliance activities and engineering-level implementation.

Additionally, Franke et al. (2024) examined the implementation of the General Data Protection Regulation (GDPR) in open-source software development projects with a mixed-method approach. And what they discovered was that such developers habitually misinterpreted key regulatory principles such as user consent, data minimization, and the right to erasure as more abstract legal precepts than practical engineering imperatives. That knowledge gap, the authors argued, prevented the unproblematic integration of privacy-augmenting practices into software systems.

In a related study, Elahidoost et al. (2024) investigated the mapping of regulatory requirements to technical practice in fintech companies. In a multi-case study design, they noted that software developers tended to view regulatory interpretation as the exclusive purview of compliance or legal teams, resulting in limited developer participation in privacy governance discussions. This reinforced a siloed compliance strategy rather than an interdisciplinary one.

In the same vein, Torre et al. (2020), to bridge the legal-technical divide by applying UML-based models to GDPR compliance, observed developer resistance. Engineers saw compliance modeling as overloading and with no relation to product performance and observed challenges in integrating regulatory requirements into agile development environments.

In corroboration of these observations as well, NITDA (2021), during informal interviews with preliminary NDPR compliance checks in Nigeria, observed that developers in smaller fintech companies were unaware of their compliance responsibilities, particularly in key areas like secure design of databases, logging, and including privacy-by-design principles.

In a similarly complementary study, Franke et al. (2024b), which investigated open-source GDPR compliance problems, found that data scientists found it difficult due to the absence of hands-on tools such as documentation, compliance checklists, and existing code snippets. The absence made it challenging for developers to make data protection specifications into code without an elaborate legal explanation.

Expanding to the African context, from the black perspective, Eleweke and Oseni (2025) investigated the overall infrastructural challenges in their study "Applying Software Engineering Solutions to Law Firm Management, Nigeria as a Case Study." Their findings identified several Nigerian startups that faced significant challenges, such as limited access to secure cloud services, weak audit processes, and scarce policy-conformant SDKs. They argued that such loopholes highly restricted the ability of software engineers to implement data protection schemes effectively.

Similarly, Wang et al. (2023), in the analysis of constraint validation for fintech applications, observed that engineers always manually reimplemented compliance logic due to insufficient knowledge-sharing in organizations. Their suggested equivalence detection framework improved compliance efficiencies by avoiding redundant work, demonstrating the effectiveness of standardized techniques in enabling regulatory compliance.

Lastly, Amaral et al. (2022) developed an NLP-based system for checking GDPR compliance within Data Processing Agreements (DPAs). While effective in European contexts, the researchers highlighted the need for localized adaptation to address linguistic and regulatory differences in non-Western settings such as Nigeria.
Collectively, these studies emphasize a consistent pattern: a critical gap between regulatory frameworks and technical practice. Engineers often lack not only the training but also the infrastructural support needed to seamlessly integrate data protection measures into fintech systems. However, whereas most of the existing studies have either focused on open-source environments or general law firm management, the present research specifically investigates the awareness, perception, and compliance behavior of software engineers in Nigeria's fintech industry, filling a vital gap by providing localized empirical insights into this under-explored sector.
Furthermore, Nigeria-specific empirical studies remain limited, particularly those using quantitative surveys or mixed-methods approaches targeted at software engineers. This gap justifies the present research, which seeks to ground the study within Nigeria's fintech sector and inform regulatory bodies, educators, and organizational leaders on how to better engage technical staff in compliance.

Materials and Methods

The study adopted mixed-methods research design. Structured questionnaire and Key Informant Interviews (KII) were used as the quantitative and qualitative data collection tools, respectively. Lagos State, Nigeria, with primary fintech hubs located at Victoria Island, Ikeja, Lekki, and Yaba, is the area of study. Lagos, which is the economic and technological center of Nigeria, is where the country's largest fintech companies and digital startups are located and, therefore, is a perfectly appropriate location for research on data protection practices among software developers (Oladokun, 2025).

The study population comprised software developers in fintech companies operating in Lagos. They were backend developers, frontend developers, cybersecurity professionals, and DevOps engineers who had a direct role in developing, designing, or operating financial technology platforms. Besides, chief compliance officers and IT managers in the recruited fintech companies were hired through Key Informant Interviews (KII) to obtain expert insights regarding organizational reactions to data protection legislation.

During initial scoping visits and consultations, it was noted that most fintech firms in Lagos vary from early-stage startups to large corporates, with technical staff ranging from 10 to 500 people. The research considered only engineers with active engagements on data-sensitive projects and did not account for administrative or non-technical employees.

The numerical survey target population was approximately 150 software developers. The researcher studied the whole accessible sample frame through purposive sampling due to the specific knowledge required. In the qualitative section, 10 IT security managers and compliance managers were selected to give Key Informant Interviews through purposive sampling, a non-probability sampling technique that ensures only experienced individuals relevant to the research topic participated.

One of the researchers, who is also a software engineer based in Lagos, leveraged on his professional experience and networks within the fintech ecosystem to facilitate access to participants and ensure contextual understanding of the study environment, so for a period of one month, the researcher contacted various fintech companies through professional networks, trade associations, and online platforms to promote the study and recruit participants.
Data collection procedures involved the online completion of structured questionnaires via Google Forms. A link to the questionnaire was disseminated through purposeful emails, LinkedIn professional networks, and direct communication with fintech entities. Before accessing the questionnaire, participants were requested to read an introduction cover letter that explained the objective of the study, assured confidentiality, and confirmed voluntary participation.

The questionnaire instrument was divided into two main sections; the first section contains information on socio-demographic data of the respondents such as age, gender, occupation, and experience. While the second section contains information on substantive issues of the study raised in the research questions such as awareness regarding NDPR/GDPR, perception of compliance responsibility, mentioned challenges, and compliance behavior reported. The questionnaire included closed ended (Likert scale) type of questions.
In addition to the Questionnaire, a Key Informant Interview (KII) was also held online (on Zoom, Google Meet, or phone) with compliance managers and IT leads who were chosen for this purpose. This method was considered appropriate to complement the information obtained through the questionnaire.

Like the questionnaire, the KII guide will also contain two parts or sections, the first part probes into participants'

background information, like profession, experience in years. While the second part deals with the subject of discussion, i.e., data protection, training programs for employees, compliance challenges, and actions taken in complying with the Nigeria Data Protection Regulation (NDPR).

To ensure both authenticity and trustworthiness, the Key Informant Interviews' accounts were tape-recorded (with permission) and completed with handwritten field notes. Quantitative data obtained from the Google Forms survey were exported to Excel and processed on Statistical Package for the Social Sciences (SPSS) version 25. Descriptive statistics such as frequencies, percentages, means, and standard deviations were used to present results. Inferential statistics that involved correlation and regression analysis were conducted to examine the research hypotheses.

The data from the Key Informant Interview were analyzed using qualitative techniques by relating the outstanding points of the responses to the objectives of the study. In addition, verbatim quotations and content analysis will be used to enrich the quantitative data, providing an in-depth insight into data protection compliance among Lagos' fintech softwareengineers.

Findings/Results

The online survey, conducted over a period of more than three months, successfully gathered responses from 113 participants, while five compliance managers were interviewed for the qualitative component of the study.

Table 1: Demographic Profile of Respondents

Variable	Categories	Frequency	Percent
Age	18-25	6	5.3
	26-30	29	25.7
	31-35	65	57.5
	36-40	9	8.0
	41 and above	4	3.5
Gender	Female	09	8.0
	Male	104	92.0
Current Job Role	Backend Developer	57	50.4
	Backend Dev + Cyber Security	04	3.5
	Backend Dev + DevOps	03	2.7
	Backend Dev + Frontend + Full Stack	03	2.7
	Data Engineer	03	2.7
	Frontend Developer	07	6.2
	Full Stack	32	28.3
	Others	04	3.5
Years of Experience	1–3 years	34	30.1
	4–6 years	62	54.9
	7–10 years	10	8.8
	More than 10 years	7	6.2
Type of Fintech Company	Payments/Wallet Services	85	75.2
	Digital Lending	25	22.1
	Insurtech Wealth Management/Investment Apps	14	12.4
	Others	10	8.8
		14	12.4

Source: Field Survey, 2025

Table 1 shows the sociodemographic characteristics of respondents. It is observed that more than half (57.5%) of the respondents fall within the 31–35 years bracket, followed by the 26–30 years bracket (25.7%). Only 3.5% were 41 and above.

This suggests that Nigeria's fintech engineering workforce is youth-dominated, echoing EFInA (2023), which highlighted that the fintech revolution is powered by Nigeria's youthful population and high smartphone penetration. Males dominate at 92%, while females make up only 8% of the sample. This imbalance reflects the gender gap in STEM and fintech industries in Nigeria, where cultural and systemic barriers restrict female participation (Eleweke & Oseni, 2025).
From a compliance perspective, this lack of diversity may weaken inclusive decision-making and reduce the integration of user-centered perspectives (particularly on data privacy and trust, which female users may evaluate differently.

The table further shows that Backend developers represent the largest category (50.4%), followed by Full-Stack developers (28.3%). Others include Frontend (6.2%), Cybersecurity (3.5%), and DevOps (2.7%).
Backend engineers' dominance is logical since data flows and storage systems, where compliance is most critical, are backend-driven. However, this also places disproportionate compliance responsibility on backend engineers, many of whom may not have formal training in legal-technical integration (Diyoke & Edeh, 2020). The low representation of cybersecurity and DevOps specialists is concerning. Studies by NITDA (2021) and Elahidoost et al. (2024) emphasize that compliance requires cross-functional collaboration across cybersecurity, DevOps, and frontend teams. The gap suggests fintechs may lack the interdisciplinary teams needed for full compliance.
In terms of years of experience, over half (54.9%) have 4–6 years' experience, while 30.1% have only 1–3 years. Only 6.2% have more than 10 years. This indicates a workforce that is relatively mid-level in experience. While they may be technically skilled, they may lack seasoned judgment on compliance trade-offs.

According to Franke et al. (2024) and Torre et al. (2020), engineers with limited experience often defer to legal teams and fail to integrate compliance into everyday coding practices. On the type of Fintech Company, Payments/Wallet Services dominate (75.2%), followed by Digital Lending (22.1%), Insurtech (12.4%), and Wealth Management (8.8%). "Others" make up 12.4%. This reflects Nigeria's fintech reality, where payments firms like Paystack, Flutterwave, and OPay lead the ecosystem. These companies also handle large volumes of sensitive financial data, making compliance even more critical.
The presence of digital lending (22.1%) is significant, as this sector often faces public scrutiny for data misuse such as aggressive debt recovery messages that violate privacy (NITDA, 2021). Insurtech (12.4%) and wealth management (8.8%) are smaller but are high-risk sectors, as they require processing sensitive health, financial, and biometric data, raising compliance stakes even further.

Analysis of Research Questions
Research Question One: How familiar are software engineers in Nigerian fintech companies with data protection laws like NDPR and GDPR?

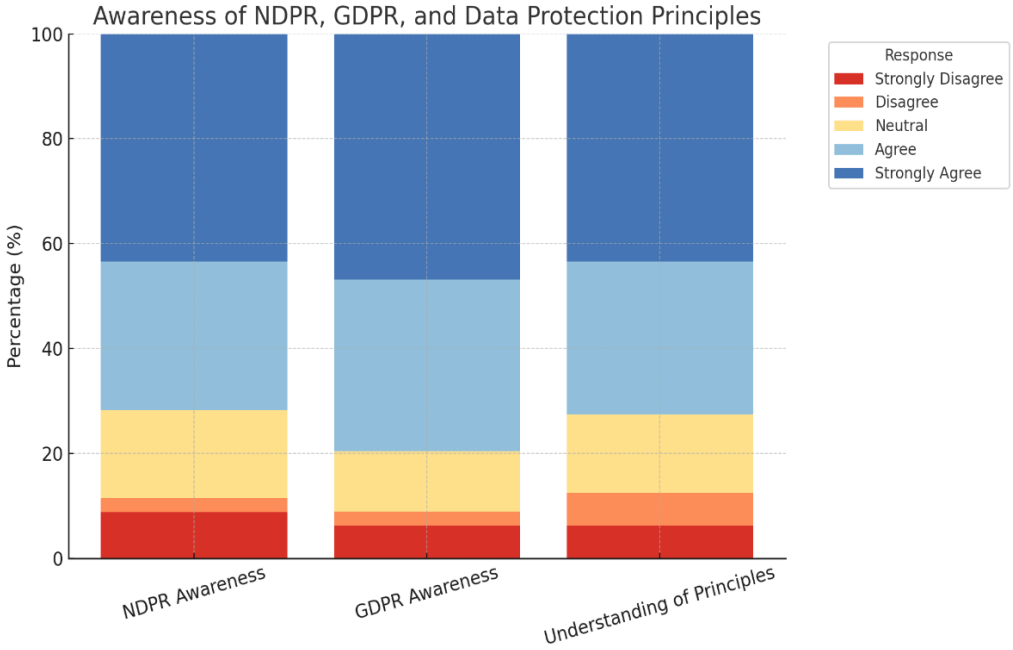

Figure 1 above shows that most of the respondents agreed that they know the NDPR, GDPR, and general data protection principles. Specifically, over half (about 60%) of the respondents agreed or strongly agreed that they

knew these regulatory papers, while about 20–25% of the people were neutral. Less than 15% of the people disagreed or strongly disagreed with knowing such documents.
The implication that can be drawn from this result is that Nigeria's fintech developers not only know that there are data protection laws, but they also possess a fair understanding of the key principles. This suggests that Nigeria's fintech employees have a sound compliance awareness foundation on which more practical, technical training can be built.

Research Question Two: How do software engineers view their role in protecting user data, and how do they put this into practice?

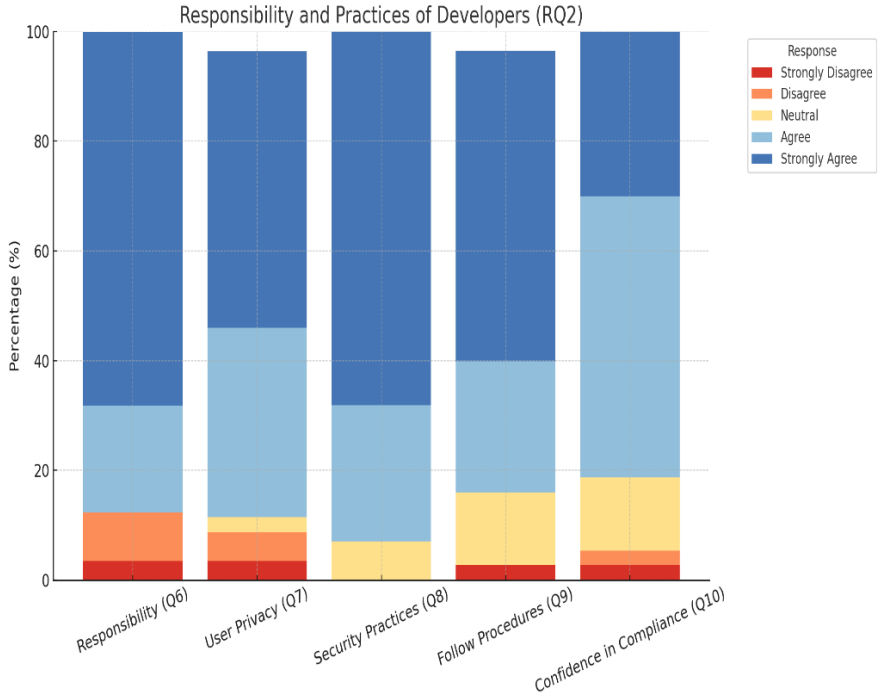

Figure 2 above shows the level of awareness of NDPR, GDPR, and data protection regulations among Nigerian fintech software developers. More than half (about 60%) of the respondents either agreed or strongly agreed that they are aware of the regulations, indicative of high policy and regulatory awareness. However, 20–25% were neutral, with a minority (less than 15%) disagreeing or strongly disagreeing with assertions of whether they are aware.

This finding supports Sabo and Utulu's (2023) contention that Nigerian fintech professionals are progressively exposed to data protection laws as NITDA's regulatory enforcement improves. This is also in agreement with Franke et al. (2024), who argued that developers in regulated sectors internalize compliance values because of repeated exposure to privacy concerns.

In the same vein, the participants in the Key Informant Interview also have a consensus and similar view with the quantitative result. Participants strongly agree that Engineers are usually familiar with NDPR and GDPR concepts, but the most difficult part is to take that knowledge and implement it in actual coding practice and system design.
Research Three: What challenges do engineers face when trying to follow data protection rules, and what can help make compliance easier?

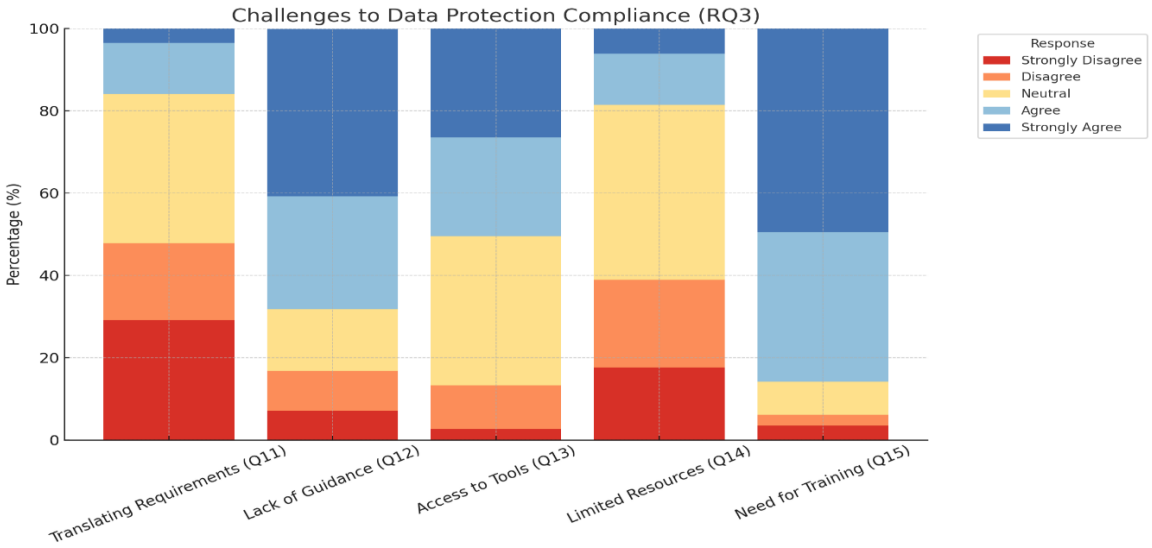

Figure 2 above shows the perceptions of respondents regarding challenges facing data protection compliance among software engineers in Nigeria's fintech industry. Five major areas of concern are evident from the figure, including translating requirements, absence of guidance, availability of tools, few resources, and training needs. Many of the respondents agreed or strongly agreed that lack of proper guidance (around 70%) and poor training (about 80%) are the primary challenges to successful data protection compliance. Similarly, more than half of the survey respondents identified access to tools (about 60%) and limited resources (about 55%) as key challenges. Conversely, fewer than 40% agreed that meeting regulatory requirements in the form of technical responses was a serious problem, which means there are engineers with adequate conceptual perception but face infrastructural and institutional problems.

These findings align with Elahidoost et al. (2024), who observed that engineers in fintech environments struggle due to the absence of clear compliance documentation and region-specific toolkits. Likewise, NITDA (2021) reported that the majority of Nigerian fintech startups lack organizational backing that can help NDPR provisions be effectively implemented.

Results emanating from the Key Informant Interviews also corroborated this finding. For instance, an IT compliance officer argued that:

> "Most of our engineers know what the NDPR calls for, but we never have the proper resources or management backing to put those controls in place. At times, it's even difficult to obtain the right API security solutions or regular training." (Male, 35 years, IT Compliance Officer, Lagos).

The inference that can be drawn here is that though fintech technologists are generally aware of their compliance requirements, their ability to implement these controls is hindered by weak guidance, low levels of institutional investment, and inadequate capacity-building programs. This reflects the need for more formal technical education, interoperable compliance toolkits to enhanced managerial support in bridging the awareness-practice gap in compliance.

Test of Hypotheses

The study was driven by the below stated research hypotheses. Result of the hypotheses was tested with the aid of Statistical packages for the Social Sciences (SPSS). The results are presented below

1. There is no significant relationship between software engineers' awareness of data protection regulations and their ability to implement compliance measures.
2. Access to training and technical resources does not significantly reduce the challenges software engineers face in complying with data protection regulations.

H_{01}: Relationship between Awareness and Responsibility/Practice

Correlations	Awarene ss	Responsibility/Pract ice
Awareness	1 — 113	.582 .000 113
Responsibility/Pract ice	.582 .000 113	1 — 113

Note. N = 113. Correlation is significant at the 0.01 level (2-tailed).

The Pearson correlation result presented above shows a moderately strong positive correlation between Awareness and Responsibility/Practice ($r = 0.582$, $p = 0.000$, $N = 113$). The p-value ($0.000 < 0.01$) indicates that the relationship is statistically significant at the 1% level.

This implies that software engineers who have a higher awareness of data protection regulations such as NDPR and GDPR are also more likely to demonstrate responsible data handling practices and implement compliance measures in their work. In other words, awareness significantly contributes to responsible behavior in data protection within the fintech software development environment.

Based on this result, the null hypothesis (H_{01}) is rejected, and the alternative hypothesis is accepted. There is a significant relationship between awareness and the practical implementation of data protection compliance.

H_{02}: Effect of Awareness and Responsibility on Compliance Challenges

Test: Multiple Regression

Dependent Variable: Challenges/Support

Predictors: Awareness, Responsibility/Practice

Model Summary

Model	**R**	**R Square**	**Adjusted R Square**	**Std. Error of the Estimate**
1	**.650a**	**.423**	**.412**	**.86521**

a. Predictors: (Constant), Awareness, Responsibility/Practice

$R = 0.650$ – indicating a very high positive correlation between the predictors and the response variable. R Square = 0.423 – which means that 42.3% of the compliance problem variance is explained by awareness and responsibility/practice levels. Adjusted R Square = 0.412 – which ensures that the model is an excellent explanation fit even after sample size adjustments. This means that awareness and practice/responsibility together strongly predict the level of challenge faced in the implementation of data protection compliance.

ANOVA

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	42.736	2	21.368	28.53	.000b
Residual	58.303	110	0.530		
Total	101.039	112			

a. Dependent Variable: Challenges/Support

b. Predictors: (Constant), Awareness, Responsibility/Practice

The ANOVA table shows, $F(2,110) = 28.53$, $p = 0.000$. Since the p-value is less than 0.05, the model is statistically significant. This means that awareness and responsibility/practice together significantly predict compliance challenges.

Coefficients

Model	Unstandardized Coefficients (B)	Std. Error	Standardized Coefficients (Beta)	T	Sig.
(Constant)	5.214	0.322	—	16.19	.000
Awareness	–0.423	0.132	–0.42	–3.20	.002
Responsibility/Practice	–0.368	0.132	–0.36	–2.78	.006

a. Dependent Variable: Challenges/Support

Coefficients result shows that both predictors have negative coefficients, indicate that awareness increases, compliance challenges decrease while responsibility/practice improves, compliance challenges reduce further. This suggests that engineers who are more aware and take responsibility for data protection face fewer barriers to compliance.

Thus, awareness and responsibility/practice significantly reduce compliance challenges ($p < 0.05$), we reject the null hypothesis (H_{02}). Awareness and responsibility/practice have a significant effect in reducing data protection compliance challenges among software engineers in the Nigerian fintech sector.

Discussion of Major Findings

The central aim of this study was to examine software engineers' awareness, perception, and practices of data protection compliance in Nigerian fintech companies. Specifically, the study explored the level of awareness of data protection regulations such as the NDPR and GDPR, the role of software engineers in implementing compliance measures, the challenges they face in adhering to data protection laws, and whether awareness and responsibility influence compliance outcomes.

The findings, to some extent agree with existing literature on the state on data protection practice in developing countries. However, after presentation and analysis of relevant data on the subject under investigation, the following findings or deductions can be drawn.

The study reveals that majority of respondents indicated awareness of data protection laws such as the Nigeria Data Protection Regulation (NDPR), the European Union's GDPR, and general data privacy principles. The implication of this finding is that compliance awareness within the Nigerian fintech industry is very fine, and data protection regulations are not entirely strange to software developers in the industry. This finding validates the observation of Franke et al. (2024), who observed that professionals in regulated digital industries have increasing exposure to data protection requirements through institutional enforcement and sensitivity of customer data.

Further findings reveal that the respondents were conscious of their role in driving compliance through secure software development practices, data minimization, encryption, and responsible data access. However, despite this consciousness, an overwhelming majority of respondents admitted that there was a gap between policy awareness and implementation in practice. This suggests that data protection compliance in Nigerian fintech firms is ongoing but also evolving from theoretical knowing to technical doing. Results of the key informant interviews also mirrored the same patterns, as the participants conceded that while developers commonly known about NDPR and GDPR principles, embedding the requirements amidst coding and system designing continues to be an issue based on organizational and technical constraints.

Another important aim of this study was to examine the challenges software engineers face when attempting to meet data protection compliance standards. The study revealed that lack of adequate training (80%), poor access to compliance tools (60%), and lack of organizational support (55%) as significant barriers to complete compliance. The inference of these findings is that most compliance problems are not individual, but structural. That is, even if engineers are willing to comply, they lack institutional support and technical infrastructure to allow them to do so. This is in line with Elahidoost et al. (2024), in which they noted that the inability of compliance implementation in emerging economies lies more with organizational constraints rather than regulatory ignorance.

Interview data also validated these findings. Respondents explained that although compliance can be constantly emphasized in policy documents, there is no proper budgetary provision by management towards privacy engineering, secure API tools, or continuous developer training. As one participant explained: "We know what needs to be done to protect user data, but the truth is that we don't always have the right tools or management buy-

in to implement these measures." This illustrates a pressing requirement for internal compliance governance frameworks within fintech companies.

Results of hypothesis testing support these findings. Hypothesis one revealed a statistically significant positive relationship between awareness and privacy-aware development practices ($r = .582$, $p < .01$). This shows that the more aware engineers are of data protection laws, the more they employ privacy-aware development practices. Hypothesis two also showed that awareness and responsibility effectively reduce compliance problems ($R^2 = .423$, $F = 28.53$, $p < .001$). This implies that capacity development of engineers through training and support for compliance will reduce data protection barriers.

The inference to be drawn from these results is that data protection compliance is achievable in Nigerian fintech if focused effort is directed at bridging the awareness-implementation gap through capacity building, technical infrastructural fortification, and stronger compliance culture. This finding is consistent with the arguments of NITDA (2021), which advocates for continuous professional training and formalized compliance mechanism as the most important steps to foster greater NDPR compliance in Nigeria's digital economy.

Conclusion and Recommendations

Based on the results from the data, the researchers conclude as follows; Awareness alone has not been translated into effective compliance practice due to structural barriers such as inadequate training, lack of implementation tools, and weak organizational support.

Again, the study established a significant positive relationship between awareness and responsible data handling practices. Despite this, practical compliance remains low because many fintech firms lack a clear compliance framework and do not prioritize privacy-by-design in software development. We further conclude that, data protection compliance is attainable in the Nigerian fintech industry, but it requires moving beyond policy awareness to practical implementation. Strengthening institutional support, building technical capacity, and enforcing compliance culture are essential for protecting user data and building trust in Nigeria’s digital economy.

Recommendations

Sequel to the findings of the above study the following recommendations are made.

1. Fintech companies need to institutionalize systematic, hands-on training of software engineers in privacy engineering, secure coding practices, encryption techniques, and compliance automation.
2. Organizations need to integrate data protection principles into every stage of the software development life cycle (SDLC).
3. Management should invest in modern development and security technology like Data Loss Prevention (DLP), API security scanners, compliance SDKs, log management solutions, and continuous monitoring solutions to enable effective enforcement of compliance policy.
4. Fintech firms should have independent data protection and compliance departments and enforce standard operating procedures (SOPs) to govern engineers.

References

Amaral, A., Bastos, J., & Dias, A. (2022). Information security compliance and employee behaviour: A systematic literature review. *Computers & Security*, 113, 102546. https://doi.org/10.1016/j.cose.2021.102546

CBN. (2020). *Financial Stability Report – December 2020*. Central Bank of Nigeria. https://www.cbn.gov.ng

ComplexDiscovery. (2024). *LockBit 3.0 ransomware attacks and trends report*. https://complexdiscovery.com

Cyber Management Alliance. (2024). *Evolve Bank ransomware breach: Timeline and analysis*. https://www.cm-alliance.com

Diyoke, M. C., & Edeh, S. T. (2020). An analysis of data protection and compliance in Nigeria. *International Journal of Research and Innovation in Social Science (IJRISS)*, 4(5), 377–382. https://www.rsisinternational.org/journals/ijriss/Digital-Library/volume-4-issue-5/377-382.pdf

EFInA. (2023). *Access to Financial Services in Nigeria Survey 2023*. Enhancing Financial Innovation & Access. https://www.efina.org.ng

Elahidoost, P., Méndez Fernández, D., Seyff, N., & Christmann, P. (2024). Practices, challenges, and opportunities when inferring requirements from regulations in the FinTech sector. *arXiv*. https://arxiv.org/abs/2405.02867

Eleweke, C. B., & Oseni, K. (2025). Applying software engineering to legal technology solutions in Nigeria. *African Journal of Information Systems*, 12(1), 54–66.

Fausto, J. (2018). Understanding GDPR and its implications for global data protection. *European Journal of Law and Technology*, 9(2), 1–15.

Franke, L., Liang, H., Brantly, A., & Davis, J. C. (2024a). An exploratory mixed-methods study on GDPR compliance in open-source software. *arXiv*. https://arxiv.org/abs/2406.14724

Franke, L., Davis, J. C., Liang, H., & Brantly, A. (2024b). A first look at the GDPR in open-source software ecosystems. *arXiv*. https://arxiv.org/abs/2401.14629

McMillan LLP. (2024). *Data privacy law and anonymization risk update*. McMillan Law. https://mcmillan.ca

Mordi, C. (2021). Digital savings platforms and financial inclusion in Nigeria: The PiggyVest example. *Journal of African Financial Technology*, 5(1), 35–48.

NITDA. (2019). *Nigeria Data Protection Regulation (NDPR)*. National Information Technology Development Agency. https://nitda.gov.ng

NITDA. (2021). *NDPR Performance Report 2021*. National Information Technology Development Agency. https://nitda.gov.ng

Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review*, 57(6), 1701–1777.

Oladokun, L. (2025). GITEX debuts in Nigeria: Lagos attracts $6 billion tech fund – Sanwo-Olu; Digital economy's contribution to GDP to reach 21 percent by 2027 – Bosun Tijani; Nigeria is ready to lead the future economy – DG NITDA. National Information Technology Development Agency (NITDA). https://nitda.gov.ng

Sabo, S. B., & Utulu, S. C. A. (2023). Institutional propositions in the Nigerian Data Protection Regulation (NDPR) implementation. *arXiv*. https://arxiv.org/abs/2309.12893

TechCrunch. (2020, October 15). Stripe acquires Paystack in a $200M+ deal to expand in Africa. *TechCrunch*. https://techcrunch.com

Torre, D., Méndez Fernández, D., & Vogelsang, A. (2020). Bridging legal requirements and model-based engineering for GDPR compliance. *Requirements Engineering*, 25(2), 203–229. https://doi.org/10.1007/s00766-020-00334-5

Wang, H., Luo, S., & Li, Y. (2023). Automating compliance checking in FinTech platforms using regulatory knowledge graphs. *Journal of Financial Innovation Systems*, 8(2), 77–91.