PrivaLex Advisory
...Compliance Redefined, Privacy Secured

Data Protection Compliance Annual Report 2025

An Analysis of Data Protection Compliance in Nigeria: Awareness, Challenges, and Success Factors.

www.privalexadvisory.com

contact@privalexadvisory.com

Table of Contents

What's Inside?

Executive Summary

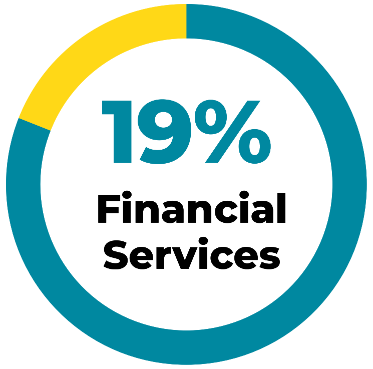
An Analysis of Data Protection Compliance in Nigeria: Awareness, Challenges, and Success Factors

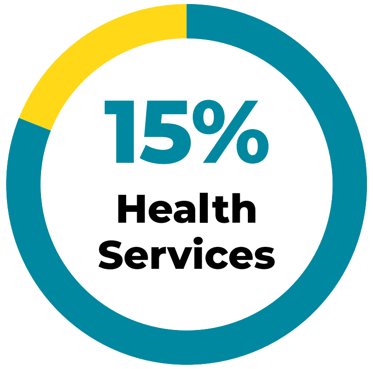
In an era marked by rapid digital transformation, robust data protection compliance is essential to safeguard privacy and foster trust among consumers and stakeholders of digital platforms. In Nigeria, the enactment of the Nigeria Data Protection Regulation (NDPR) 2019 and the Nigeria Data Protection Act (NDPA) 2023 signify crucial steps in establishing a comprehensive framework for data privacy and compliance.

This report evaluated responses to a survey analyzing awareness, challenges, and success factors related to implementing these standards across various sectors. The key areas covered included organisational roles, data protection policies, awareness programs, privacy risk management, and challenges in adhering to regulations.

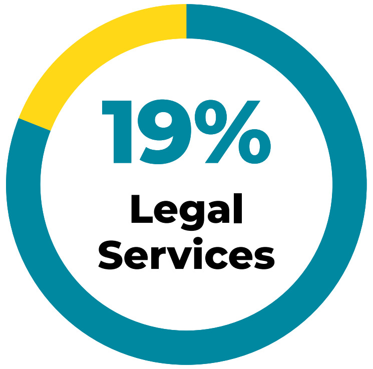
This report also highlights varying levels of compliance and readiness among organisations in Nigeria. While some organisations are adopting proactive measures such as regular DPIAs, third-party risk mitigation, and automation tools, challenges remain in areas such as integrating privacy into enterprise risk management and addressing gaps in training and awareness. Consumer attitudes and aligning organisational strategies accordingly remains a key area for improvement.

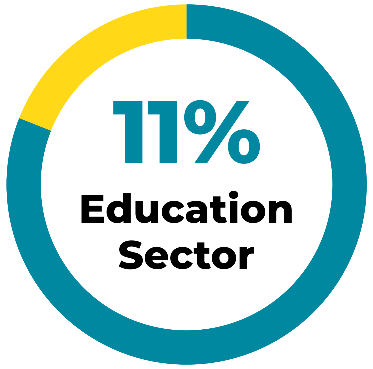
The survey garnered participation from industries including financial services, health, legal, education, marketing, oil and gas, consulting, manufacturing, NGOs, telecommunications, and technology. Notably, the



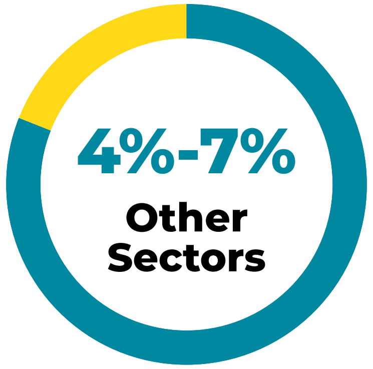


Financial services (19%), health services (15%).





Legal services (19%), and education (11%) sectors dominated the response poll.



While other sectors contributed between 4% and 7%.

Public sector participation came from Education and Health. This report provides a basis for identifying best practices and areas where organisations and regulators can focus their efforts to strengthen data protection compliance and build trust in data privacy.

Section 1: Governance & Accountability

1. Governance and Accountability

Introduction

Effective governance and accountability structures are foundational to achieving data protection compliance. This section explores the extent to which organisations integrate data protection principles into their processes, conduct Data Protection Impact Assessments (DPIAs), manage data breaches, and maintain accountability through proper record-keeping and oversight teams. It highlights gaps in policy implementation and suggests strategies to strengthen compliance frameworks.

1.1 Integrating Data Protection in Design and Implementation

In the survey, we asked privacy professionals:

> ‘Does your organisation have policies and procedures to make sure that Data Protection issues are considered when systems services, products and business practices involving personal data are designed and implemented and that personal data is protected by default?'

Out of all respondents 59% indicated that their organisations have policies and procedures in place for privacy by design and default. 33% admitted that they lack such policies and procedures. 7% reported being unaware of whether their organisations have these measures in place. These findings underscore a significant gap between policy implementation and awareness of data protection principles across Nigerian organisations.

- Private Sector:

59%

of the respondents affirmed having policies and procedures for privacy by design and default.

36%

of the respondents reported not having such measures in place.

5%

of the respondents were unaware of their organisation's stance on the issue.

- Public Sector:

60%

of the respondents confirmed the presence of privacy by design and default measures.

20%

of the respondents indicated the absence of such measures.

20%

of the respondents were unaware of their organisation's governance status.

From the analysis, the 59% affirmative response rate across sectors indicates moderate awareness and adoption of privacy by design and default principles. However, the 33% of organisations without such measures highlights a significant gap in implementation, especially in the private sector where commercial pressure might prioritise speed and cost over compliance.

The 7% aggregate response of "unaware" and the 20% unawareness rate in the public sector signal a critical issue: insufficient training or dissemination of data protection standards within organisations.

The marginally higher affirmative response in the public sector (60% vs. 59%) suggests that government agencies may be slightly more inclined to adopt data protection measures, possibly due to increased regulatory oversight. However, the substantial proportion of public sector respondents (20%) who are unaware of their organisation's compliance raises concerns about the adequacy of enforcement and capacity-building efforts.

1.2 Conducting Data Protection Impact Assessments (DPIA)

‘Do you have a process for conducting Data Protection Impact Assessment (DPIA) on existing or potential projects?'

Overall, 48% of respondents reported having a process for conducting DPIAs on existing or potential projects, while 37% indicated they do not, and 15% were unaware of the process.

- **Private Sector:**

59%

of the respondents affirmed having DPIA processes.

36%

of the respondents admitted to lacking such processes.

5%

of the respondents were unaware of this requirement.

Public Sector:

60%

of the respondents confirmed they conduct DPIAs.

20%

of the respondent indicated they do not conduct DPIAs,

20%

of the respondents were unaware of the concept.

The higher compliance in the public sector may be attributed to regulatory mandates for government entities, while private sector organisations especially multinationals often align with international standards due to business imperatives. The lack of awareness among a notable minority highlights inadequate training and dissemination of NDPR/NDPA requirements. A substantial proportion of organisations failing to conduct DPIAs poses risks of non-compliance, leading to potential breaches and fines. Awareness campaigns and capacity-building initiatives are crucial.

1.3 Documented Data Breach Incident Management Procedures

'Do you have a documented data breach incident management procedure?'

Among respondents, 41% have documented data breach incident management procedures, 37% do not, and 22% are unaware of the need for such protocols.

- **Private Sector:**

41%

of the respondents confirmed having such procedure.

41%

of the respondents lacked having such procedure.

18%

of the respondents were unaware of such procedure.

- **Public Sector: Only**

40%

of the respondents confirmed having such protocols.

40%

of the respondents lacked such protocols.

20%

of the respondents were unaware of such protocols.

The relatively low compliance may stem from limited resources or a lack of emphasis on incident response readiness. Smaller private organisations and some public entities may struggle with implementing these frameworks. The absence of incident management procedures increases vulnerability to data breaches and regulatory penalties. This highlights the urgent need for guidelines and support from regulators.

1.4 Inclusion of Data Protection Clauses in Contracts

‘Do you include Data Protection Clauses in your Contracts or sign Data Processing Agreements with third party suppliers?'

A majority (66%) of respondents reported incorporating data protection clauses in contracts or signing Data Processing Agreements (DPAs) with third-party suppliers. However, 30% do not, and 4% were unaware of this requirement.

- **Private Sector:**

73%
of the respondents affirmed compliance.

27%
of the respondents did not affirmed compliance.

- **Public Sector:** Only

40%
of the respondents confirmed compliance.

40%
of the respondents indicated they do not confirmed compliance.

20%
of the respondents were unaware of such compliance.

The private sector's higher compliance could be linked to international contractual obligations, while public sector entities may face bureaucratic delays in updating procurement standards. Non-compliance can expose organisations to third-party data misuse, undermining trust and legal standing. Clear mandates on contract review processes are essential.

1.5 Record of Processing Activities (RoPA)

Do you maintain a record of all your processing activities?

Eighty-one percent of respondents maintain records of their processing activities, 12% do not, and 7% were unaware.

- **Private Sector:**

80%
of the respondents confirmed compliance.

15%
of the respondents confirmed non-compliance.

5%
of the respondents were unaware of such compliance.

- **Public Sector:**

80%
of the respondents confirmed compliance.

20%
of the respondents were unaware of such compliance.

The high compliance rate may reflect the straightforward nature of maintaining such records compared to other data protection requirements. Maintaining RoPAs is foundational for audits and demonstrates accountability. Expanding training on this requirement could ensure near-universal compliance.

1.6 Designated Data Protection Compliance Team

Do you have a designated team or staff responsible for your compliance with Data Protection law and processes?

Only 48% of respondents have designated teams or staff responsible for data protection, 41% do not, and 11% are unaware of this requirement.

- **Private Sector:**

50%

of the respondents affirmed having designated teams.

45%

of the respondents do not have designated teams.

5%

of the respondents were unaware of this requirement.

- **Public Sector:**

60%

of the respondents reported having teams,

20%

of the respondents reported not having teams.

20%

of the respondents were unaware of the requirement.

Resource constraints, especially in smaller organisations, may limit the establishment of dedicated teams. Public sector compliance may benefit from centralized directives. The absence of dedicated teams undermines structured compliance efforts, leaving organisations susceptible to oversight lapses with regards to fulfilling data protection obligations.

1.7 Appointment of Data Protection Compliance Organizations (DPCOs)

Have you appointed a Data Protection Compliance Organization (DPCO)?

Only 37% of respondents have appointed DPCOs, while 52% have not, and 11% were unaware of the requirement..

Private Sector:

36%

of the respondents reported compliance.

59%

of the respondents did not report compliance.

5%

of the respondents were unaware of the requirement.

- **Public Sector:**

40%

of the respondents affirmed compliance

20%

of the respondent did not affirmed compliance.

40%

of the respondents were unaware of the requirement.

Cost implications and uncertainty about DPCO roles may deter compliance, especially among smaller organisations. A lack of DPCOs diminishes expert oversight in compliance, increasing the likelihood of regulatory breaches. Awareness programs to highlight DPCO benefits could drive uptake.

1.8 How are roles and responsibilities for privacy risk management structured in your organisation?

Out of all the respondents 67% gave a response stating it is centralised, meaning that from top managers to support staff, roles are clearly defined, with designated teams handling privacy risk management and compliance, employees have different task and job roles especially geared towards privacy risk,

A smaller, yet concerning, 23% of respondents admitted that their organisations lack structured roles and responsibilities for privacy risk management or that they were unaware of such arrangements. These responses suggest significant gaps in organisational readiness and awareness, which may hinder compliance and risk mitigation efforts.

Section 2: Training & Awareness

Introduction

This section evaluates the effectiveness of training and awareness programs provided by organisations. Training and awareness play a vital role in cultivating a culture of compliance and accountability in data protection. The findings offer insights into the progress of efforts to promote data privacy within Nigerian organisations. Responses highlight the initiatives organisations are implementing to ensure employees at all levels understand their responsibilities in safeguarding personal data, complying with privacy regulations, and mitigating risks.

2.1 Organizing data protection awareness seminar for staff and customers.

This question sought to determine whether organisations have taken proactive steps to educate their staff and customers about data protection within the year 2024.

The survey findings suggest that the private sector is performing better than the public sector in organising awareness campaigns and training related to data protection. The overall result shows that more than half of the respondent organisations had trained staff and created awareness for customers on data protection, while a significant portion either didn't receive training or were unaware of its availability. However, gaps remain in both sectors.

52% of the respondents received data protection training and created awareness for customers on data protection in 2024.
37% of the respondents did not receive any data protection training or create awareness for customers in 2024.
11% were unsure if any training or awareness programs had been organised by their organisations.

Sector-Specific Insights:

Private Sector:

55%

of the respondents reported that their organisations are actively organizing awareness campaigns for customer and staff.

36%

of the respondents indicated that no such campaigns have been organised for staff or customers.

9%

of the respondents were unaware if any data protection training had been conducted for either staff or customers.

Public Sector:

40%

of the respondents stated that their organisations are organising awareness campaigns for customer and staff.

40%

of the respondents confirmed that no training has been provided for staff or customers.

20%

of the respondents were unaware if any training or campaigns had been organised for either staff or customers.

These results highlight that while the private sector is more proactive in raising awareness, there is still a lack of comprehensive efforts across both sectors. Increasing awareness campaigns and ensuring consistent training for staff and customers in both private and public organisations is essential for fostering a strong culture of data protection and compliance.

Organisations can strive to achieve data protection compliance by educating all their employees. Through data protection trainings, staff are able to understand data privacy and implement safeguards which help protect personal data which in turn creates a more secure and privacy-conscious digital environment.

On the other hand, customer awareness of data protection empowers individuals to make informed decisions about their personal information, builds trust with data processing organisations, and encourages accountability.

2.2 Training for Data Protection Team.

This question aimed to assess whether organisations have prioritised equipping their staff responsible for data protection with the necessary knowledge and skills during the year 2024.

The survey results reveal mixed levels of awareness and completion of privacy training among respondents, highlighting potential gaps in organisational data protection programs.

44% of overall respondents confirmed that privacy training had been completed by the data protection team. Another 44% were unaware if such training had occurred. 12% of respondents stated that no privacy training had been conducted for them as privacy program managers in 2024.

Sector-Specific Insights:

- **Public Sector:**

50%

of the respondents reported receiving privacy training.

50%

of the respondents indicated they had not received any training.

- **Private Sector:**

44%

of the respondents confirmed they had received training.

44%

of the respondents were unaware if training had occurred.

12%

of the respondents explicitly stated that no training had been provided.

These findings suggest significant disparities in the implementation and communication of privacy training programs, with a notable lack of awareness among majority of data protection staff. Strengthening privacy education and ensuring regular training sessions for the data protection team will be critical for improving organisational compliance and embedding a culture of data protection.

Section 3: Audit & Risk

Introduction

The audit and risk function is integral to ensuring compliance with data protection regulations. It involves systematically evaluating an organisation's data handling practices, policies, and systems to identify vulnerabilities and ensure adherence to legal and regulatory requirements. In this section, we evaluated the risk management culture and practices performed within organisations to identify, analyse, and mitigate potential threats to personal data. This section is particularly an important function, because it helps organisations proactively manage privacy risks, and address gaps in compliance thereby building trust with stakeholders and reducing the likelihood of data breaches or regulatory penalties.

3.1 Privacy Risk Integration

This question sought to determine whether an organisation's approach to managing privacy risks is embedded within its broader Enterprise Risk Management (ERM) program. Integration would indicate that privacy risks are treated as a critical aspect of overall organisational risk, alongside financial, operational, and reputational risks. The survey findings indicate that a significant majority of organisations have not integrated privacy management into their risk management frameworks.

- 67% of overall respondents stated that privacy management is not part of their organisation's risk management program.

- Only 33% affirmed that privacy has been incorporated to the broader risk management program with their organisation.

Sector-Specific Insights:

- Private Sector

71.5%

of the respondents reported that privacy risk was not included in their organisation's overall risk program.

28.5%

of the respondents indicated that privacy has been incorporated in their organisation's overall risk program.

- Public Sector:

50%

of the respondents stated that privacy risk has not been incorporated in their organisation's overall risk program.

50%

of the respondents confirmed that privacy is part of their organisation'soverall risk program.

These results highlight a critical gap in addressing privacy as a fundamental aspect of risk management. Incorporating privacy management into overall risk programs is essential for mitigating potential threats, ensuring compliance with data protection regulations, and fostering trust with stakeholders. Organisations need to prioritise privacy as a core element of their risk strategy to achieve more robust and comprehensive risk management.

3.2 Public Disclosure of Privacy Risk Management Efforts.

This question aimed to determine whether organisations share details about their privacy risk management activities with external stakeholders. Public disclosure might include publishing reports, policies, or updates on how the organisation identifies, evaluates, and mitigates privacy risks.

The survey results reveal the following findings regarding the publication of risk management activities:

Overall, 77% of respondents indicated that they do not publish any information on their risk management activities. While 23% reported that they do share reports on their privacy risk management efforts.

Sector-Specific Insights:

- **Private Sector:**

86%

of the respondents stated that they do not publish information on their risk management activities,

14%

of the respondents confirmed sharing reports on their risk management efforts.

- **Public Sector:**

50%

of the respondents stating that they do not publish any information

50%

of the respondents declared that they publish reports on their risk management efforts.

The numbers suggest a few key insights about the approach to risk management and transparency across sectors:

a. **Lack of Transparency in Risk Management:** This indicates that most organisations, whether in the private or public sector, are not openly sharing their efforts in managing privacy risks. This could suggest a reluctance or lack of focus on demonstrating transparency in privacy practices.

b. **Private Sector Reluctance to Publish Risk Management Information:** This could be due to concerns over protecting sensitive information, potential legal or regulatory implications, or simply a lower priority on communicating these efforts externally.

c. **Proactive Risk Management Can Build Trust:** The 23% of the overall respondent organisations that do publish information on their risk management activities, particularly those in the public sector (50% of their respondents), show that sharing such efforts can help build trust with customers and partners.

It suggests that organisations which prioritise transparency in risk management are likely more committed to privacy protection and are actively working to establish credibility and trustworthiness.

While some organisations are taking a proactive approach by sharing their risk management activities, the majority are not, pointing to a potential gap in transparency that should be addressed by the regulators in partnership with organisations to foster greater trust in privacy practices.

3.3 Established Privacy Risk Appetite

This question sought to assess whether the organisation has clearly defined its privacy risk appetite—the level of risk it is willing to accept while pursuing its objectives involving personal data. An established privacy risk appetite indicates that an organisation has set boundaries for managing privacy risks, balancing compliance, operational needs, and innovation.

The survey results on the establishment of a privacy risk appetite reveal the following:

- **55% of overall respondents have an established privacy risk appetite,**
- **While 45% do not have a defined privacy risk appetite.**

Sector-Specific Insights:

- **Private Sector:**

57%

of the respondents have established an organisational privacy risk appetite.

43%

of the respondents have not established an organisational privacy risk appetite.

- **Public Sector:**

50%

of the respondents stated that they had established a privacy risk appetite.

50%

of the respondents stated that they had not established a privacy risk appetite.

These numbers suggest that while a majority of overall respondent organisations (55%) have defined their approach to privacy risk, nearly half of respondents still lack a clear risk appetite. The private sector shows a slightly higher inclination to establish a risk appetite compared to the public sector, where the split is even.

This could imply that private sector organisations may be more proactive in formalizing their approach to privacy risk management, while the public sector may still be in the process of defining or formalizing their risk tolerance.

Below are some steps to take in order to establish a Privacy Risk Appetite

Based on the survey findings, organisations can take the following steps to establish or refine their privacy risk appetite:

1. **Assess Current Risk Management Practices:** Conduct an internal audit to evaluate how privacy risks are currently being managed. This includes reviewing policies, practices, and any existing risk assessments.
2. **Engage Stakeholders:** Involve key stakeholders—such as legal, compliance, IT, and executive leadership—in discussions to define the organisation's tolerance for privacy risks. This can help ensure that the risk appetite aligns with organisational goals and compliance requirements.
3. **Align with Legal and Regulatory** Requirements: Organisations should consider industry regulations when defining their privacy risk appetite. This ensures that the organisation remains compliant while managing risks.
4. **Define Clear Metrics and Tolerance Levels:** Establish specific metrics (e.g., frequency of data breaches, compliance failures) to monitor privacy risk. Determine acceptable levels of risk, such as what constitutes a "tolerable" breach and what steps must be taken to prevent it.
5. **Document and Communicate the Risk Appetite:** Once defined, the risk appetite should be documented clearly and communicated across the organisation. This ensures that all teams understand the boundaries of acceptable risk and how to operate within them.
6. **Regularly Review and Update:** Risk appetites are not static; they should be reviewed and adjusted regularly to account for changes in the regulatory landscape, business goals, and emerging privacy risks.

3.4 Compliance Audit Returns Filing with NDPC.

This question sought to determine whether organisations submit their annual compliance audit returns as mandated by the Nigeria Data Protection Commission. Filing these returns typically involves reporting on the organisation's adherence to data protection regulations, including the implementation of required privacy measures, risk management practices, and any incidents or breaches that may have occurred.

The findings reveal significant gaps in compliance with the Nigeria Data Protection Act (NDPA) across both private and public sectors:

- 41% of overall respondents confirmed that their organisations filed audit returns with the Commission, while another 37% stated they did not. Alarmingly, 22% did not know if their audit returns were filed, highlighting widespread uncertainty and lack of clarity within organisations.

These results support reports about the ineffectiveness of regulatory efforts to enhance compliance, with many organisations failing to adhere to legislative requirements due to weak enforcement mechanisms:

Sector-Specific Insights:

- ## Private Sector

41%

of the respondents indicated their organisations were compliant with the annual audit filing requirements.

37%

of the respondents admitted non-compliance with the audit filing requirement.

22%

of the respondents did not know whether their organisation was compliant with the audit filing requirement.

- ## Public Sector Compliance:

40%

of the respondents stated their organisations were compliant.

20%

of the respondents acknowledged non-compliance with the audit filing requirement.

40%

of the respondents did not know whether their organisations were compliant with the audit filing requirement.

These figures underscore a critical issue: weak enforcement and lack of awareness are major barriers to achieving compliance with the NDPA. Addressing these challenges will require more robust regulatory oversight, greater enforcement efforts, and enhanced education and communication from the Nigeria Data Protection Commission (NDPC).

3.5 Third Party Processor Risk Management.

This question sought to understand the measures organisations have implemented to manage and mitigate risks associated with **third-party data processing activities.** Third parties, such as vendors, service providers, or contractors, often handle sensitive data on behalf of the organisation, which creates potential privacy and security risks.
The survey results reveal significant variability in third-party risk management practices. While some organisations have established strong measures, others need to address gaps in awareness, communication, and formal processes to reduce risks and comply with data protection laws.
The results revealed the following:

1. Uncertainty Among Respondents:

20%

of the respondents expressed uncertainty about the measures their organisations had in place to address third-party risks. This suggests a potential lack of communication or transparency within these organisations regarding data protection policies and practices.

2. No Process in Place:

30%

of the respondents stated that their organisations had no formal process to mitigate third-party risks. This indicates a significant gap in compliance, as third-party risks are a critical component of data protection regulations.
.

3. Existing Measures in Some Organizations:

50%

of the respondents whose organisations had measures in place reported the following practices:

o Awareness of Information Privacy: Efforts to ensure staff members are educated on the importance of information privacy, which helps prevent unintentional data breaches.
o Employee Policies: Policies designed to prevent employees from inadvertently exposing data to third parties.
o Contracts and Audits: Use of strict contractual agreements, regular audits, and compliance checks to manage and monitor third-party data processing risks.

The use of contracts, audits, and staff awareness highlights the critical role third-party risk management plays in ensuring that data protection extends beyond the organization's immediate control. Organisations without measures or with uncertain respondents are at risk of **non-compliance with data protection regulations.**

3.6 Management Support for Data Protection.

This question aimed to assess whether **senior management** within the organisation actively supports and prioritises **data protection activities.** Support from management is crucial for the successful implementation of data protection policies, ensuring that adequate resources, budgets, and attention are dedicated to compliance efforts.

The survey responses regarding management support for data protection activities reveal notable insights into organisational leadership's role in fostering a culture of data privacy and security.

Overall Responses:

- 78% of overall respondents stated that their management supported data protection activities, indicating a strong level of commitment in the majority of organisations.
- 15% of overall respondents said their management did not support data protection activities, highlighting areas where leadership needs to prioritise data protection.
- 7% were unsure about their management's support, suggesting a potential gap in communication or visibility regarding leadership initiatives.

Sector-Specific Insights:

- Private Sector:

82%

of the respondents reported management support, showing a robust focus on data protection within this sector.

13%

of the respondents said their management does not support these activities, indicating some resistance or lack of prioritization in a minority of organisations.

5%

of the respondents were unsure, reflecting slightly better communication and clarity compared to the public sector.

- Public Sector:

60%

of the respondents reported that their management supported data protection activities.

20%

of the respondents said their management did not support data protection activities.

20%

of the respondents were unsure, signalling a need for improvement in leadership focus and communication.

3.7 Communication of Privacy Risk Management Strategy to staff.

This question explored the methods and strategies that organisations use to communicate their privacy risk management efforts to internal stakeholders, such as employees, managers, or board members. Effective communication ensures that everyone within the organisation understands the importance of privacy, their roles in mitigating risks, and the measures in place to protect data.

The survey responses reveal a spectrum of practices in how organisations communicate privacy risk management efforts internally. While some have established robust strategies, others lack adequate communication, leading to gaps in awareness and engagement. By adopting consistent, transparent, and varied communication approaches, organisations can ensure that privacy risk management becomes a shared responsibility across all internal stakeholders.

The results revealed the following:

No Communication:

15%

of the respondents indicated that their organsations do not communicate efforts regarding privacy risk management internally. This reveals a critical gap in fostering awareness and engagement among stakeholders.

Uncertainty:

20%

of the respondents were "not sure" and this highlights a lack of clarity or visibility regarding organisational communication efforts. This could be as a result of insufficient transparency or inconsistent communication practices.

Existing Measures in Some Organisations:

65%

of the respondents whose organizations had measures in place reported the following practices:

o **Communication via Regulatory Fulfillment and Seminars:** Their organisations rely on fulfilling regulatory requirements and seminars to communicate about privacy risk management.

o **Regular Training, Updates, and Policy Briefings:** Their organisations provide regular training, updates, and policy briefings demonstrating a structured and proactive approach to internal communication.

o **Awareness Campaigns:** They also used awareness campaigns to build a culture of data protection and privacy awareness, going beyond policy updates to actively engaging employees.

o **Regular Communications (Comms):** to integrate privacy risk management into daily operations and organisational dialogue.

3.8 Preparation for technological advancement with the emergence of AI, and other Trends

This question sought to understand how organisations are proactively addressing **emerging privacy risks** associated with technologies like **artificial intelligence (AI),** and other evolving trends. It evaluated whether organisations are anticipating these challenges and implementing measures to manage them effectively.

The survey findings highlight a significant disparity in organisational preparedness for emerging trends such as AI, and other technological advancements:

Key Findings:

1. Limited Overall Preparedness:

65%

of the respondents reported that their organisations are **not preparing** for the adoption of AI, or similar trends. This indicates a general lack of strategic focus on emerging technologies across many organisations.

35%

of the respondents noted that their organisations are actively investing in tools, training, and AI processing documentation to manage these advancements.

2. Private Sector Leadership:

50%

of the respondents stated their organisations are preparing for these technological shifts, demonstrating a more proactive approach compared to the public sector.

3. Public Sector Lagging Behind:

20%

of the respondents reported efforts towards embracing these changes, suggesting slower adoption and readiness in governmental or public institutions.

The lack of preparation by the majority of organisations could place them at a competitive disadvantage, particularly as AI and emerging technologies are expected to become integral to operational efficiency and innovation. Organisations that delay preparations for AI and emerging technologies may face challenges ensuring compliance with regulatory requirements governing these technologies. The NDPC, as a regulator, should prioritise promoting the significance of preparing for AI and technological trends by facilitating industry forums, workshops, and cross-sector collaborations. Additionally, it is essential to develop a framework that enables and governs the use of AI, ensuring alignment and consistency across all sectors in Nigeria.

3.9 Use of Privacy Tools for Privacy Risk Management.

This question aimed to determine and gauge whether organisation utilises automated tools to identify, monitor, and mitigate privacy risks.

The survey findings show that organisations are relying on manual means for the management of data protection organisations.

The results revealed the following:

Majority of Organisations are without privacy tools:

70%

of the respondents reported that their organisations have not acquired any privacy tools to manage privacy risks. This indicates a significant gap in leveraging technology for effective privacy risk management.

Organizations Using Privacy Tools:

30%

of the respondents stated their organizations have adopted privacy tools. Popular tools mentioned include OneTrust and Cealed.

The low adoption rate may stem from resource constraints or a lack of awareness about the availability and benefits of privacy tools. Encouraging widespread adoption of privacy tools will be critical for strengthening overall compliance and data protection efforts.

Section 4: Data Processing

Introduction

Understanding and managing the lifecycle of personal data are critical components of compliance. This section delves into how organisations identify data collection points, process data securely, and maintain transparency with stakeholders. It also examines disparities in operational capacities and suggests targeted interventions to address non-compliance.

4.1 Identifying Collection Points for Personal Data

Has your organisation identified all the collection points for the personal data it uses?

The survey revealed that 74% of organisations affirmed that they had identified all personal data collection points, while 24% admitted they had not.

This overall result suggests that while a significant majority have made strides toward compliance, nearly a quarter of organisations are still lagging. These disparities may point to varying levels of awareness, resource allocation, and operational capacity within different sectors.

Private Sector:

73%

of the respondents indicated they had identified all data collection points,

27%

of the respondents reported they had not identified no data collection point.

The private sector's relatively high rate of compliance may stem from its need to maintain customer trust, ensure competitive advantage, and avoid potential penalties for non-compliance. Many private organisations, especially those involved in data-driven industries such as technology, finance, and e-commerce, recognise the strategic importance of aligning with data protection standards.

However, the 27% non-compliance rate signals challenges such as inadequate resources, lack of technical expertise, and insufficient prioritisation of data protection. Smaller businesses may struggle with these issues, as they often lack the financial and human capital to invest in comprehensive privacy governance frameworks.

Public Sector:

In the public sector, the survey results were slightly more positive, with

80%

of the respondents confirmed their organizations had identified all data collection points.

20%

of the respondents acknowledged they had not identified no data collection point.

This higher compliance rate can be attributed to recent government efforts to align public institutions with the NDPR 2019 and NDPA 2023 mandates. Public sector entities often handle sensitive data and are therefore subject to heightened scrutiny, which has likely spurred initiatives to enhance compliance.

Nonetheless, the 20% non-compliance rate in the public sector highlights systemic challenges, including bureaucratic inefficiencies, limited funding for data protection programs, and outdated technological infrastructure.

In some cases, public institutions may face difficulties in mapping complex and fragmented data flows, particularly in large organisations with decentralised operations.

4.2 Personal Data Lifecycle Management

How does your organisation identify, map, and manage personal data throughout its lifecycle?

Organisations reported varying approaches to identifying, mapping, and managing personal data throughout its lifecycle:

- Some organisations track, classify, and secure personal data at every stage using audits and comprehensive data management systems. These systems enable structured oversight and help mitigate risks associated with data handling.
- Many respondents have adopted a data mapping structure as a cultural norm, ensuring consistent and proactive data management across departments.
- A few uses traditional methods, such as record books and application software, for data documentation and management.

- Certain participants highlighted the use of filing systems, emphasising manual data handling processes.
- Some organisations rely on "champions" within their teams to map data effectively, leveraging internal expertise to uphold data protection standards.
- Others admitted their processes are still under development, reflecting ongoing efforts to establish robust data management practices.
- Notably, a segment of respondents was unaware of their organisation's data lifecycle management practices, indicating significant room for improvement in awareness and training.

Section 5: Security

Introduction

Data security underpins the trustworthiness of any compliance framework. This section examines the extent to which organisations implement security measures to safeguard personal data. It explores current practices in data encryption, access controls, and incident response.

5.1 What technical and organisational measures are in place to protect personal data?

From the responses, below are the detailed technical and organisational measures implemented to protect personal data across the industries engaged in Nigeria:

- **Data Encryption:** Robust encryption protocols are used for data in transit and at rest to ensure personal data security.
- **Access Control:** Role-based access controls and multi-factor authentication (MFA) are enforced to limit data access to authorised personnel.
- **Data Backup and Recovery:** Personal data is regularly backed up and stored securely, supported by disaster recovery plans.
- **Security Monitoring:** Advanced real-time monitoring tools and regular vulnerability assessments are utilised.
- **Privacy Policies and Employee Training:** Clear privacy policies are communicated, and employees receive regular training under the Nigeria Data Protection Act.

- **Data Minimization:** Organisations enforce data retention schedules and collect only necessary personal data.
- **Incident Response Plan:** Detailed plans outline breach response steps, including notifications to affected parties and regulators.
- **Third-Party Risk Management:** Third-party data protection practices are assessed and monitored for compliance.
- **Physical Security:** Secure storage measures for physical documents containing personal data are in place.
- **Threat Intelligence:** Vulnerability management, secure remote access, web filtering, and logging and monitoring systems are employed.
- **Specialised Training:** Periodic cybersecurity seminars and ongoing data protection education are conducted.
- **Policies and Practices:** Encryption, firewalls, endpoint security, and DPIA policies are standard measures.
- **Password Management:** Strong passwords, two-factor authentication (2FA), and device security tools like BitLocker are used.

Section 6: Challenges in Data Protection Compliance

Introduction

Data protection compliance presents numerous challenges for organisations as they navigate complex regulations, evolving technologies, and growing privacy concerns. Balancing legal requirements with operational efficiency, managing emerging risks like AI and emerging technologies, and fostering a culture of accountability are just a few of the hurdles that organisations face. In this section, we reviewed the unique challenges faced by Nigerian businesses in response to their compliance responsibilities.

6.1 Customer Perception of Privacy and its effect in Business.

This question aimed to understand whether consumers are generally concerned about their privacy and how that concern, or lack thereof, impacts the organisation's approach to data protection, transparency, and compliance. The survey responses on customer reactions towards privacy in Nigeria reveal significant insights into public awareness and attitudes regarding data protection. The prevailing responses were the following:

Concern for Data Protection:

- Majority of the respondents said that it was only a lower percentage of their customers, that were explicitly concerned about their data being protected. While there is some awareness of the need for data privacy, it appears limited in scope and depth.

Lack of Awareness of Privacy Measures:

· A significant number of the respondents said that many of their customers were unaware of measures their organisations have in place to ensure data privacy. This suggests a communication gap between organisations and their customers regarding data protection practices and policies.

Indifference and Nonchalance:

· The majority of Nigerians have been described by our respondents as nonchalant or indifferent about data privacy. This indifference likely stems from:

o **Lack of understanding:** Many customers are not educated on what data privacy entails.

o **Limited awareness of risks:** Perception of the potential consequences of poor data protection.

Most of the respondents have stated that customer indifference has reduced the pressure on their organisations to prioritise compliance with data protection laws. As a result, they fear that senior management may perceive the role of the data protection team as less critical, potentially leading to lower levels of compliance.

The general indifference and lack of understanding among customers highlight a significant **awareness gap** regarding data privacy in Nigeria. And this can hinder the effectiveness of privacy-related initiatives and leave customers vulnerable to data breaches or misuse.

6.2 Top Privacy risks faced within Nigerian Organisations.

This question asks organisations to identify and prioritise the most significant privacy risks they currently face. The findings of this study highlight that all organisations, regardless of size or industry, face privacy risks when handling personal data. While the specific challenges may vary, key privacy risk categories identified by participants include:

1. **Data Leakages:** Accidental or intentional exposure of sensitive information which leads to significant reputational damage and legal consequences.
2. **Insider Threats:** Employees or contractors with access to sensitive data misusing or compromising information, either maliciously or unintentionally.
3. **The Use of AI:** With AI technologies increasingly being used to process personal data, concerns about data privacy and the ethical use of AI are growing. The concerns are around AI regulation, data misuse and biased decision-making.
4. **Inadequate Data Security Management:** Weaknesses in their data protection practices, such as lack of encryption, inadequate access controls, and outdated security protocols.

The above risks identified, can be categorized into **human risks, technological risks, and regulatory risks**, se breaches.

If these risks are not effectively managed, they can pose significant threats to both the organisation and its customers. A lack of trust in the organisation's ability to protect or lawfully use personal information may lead customers to avoid doing business with companies they perceive as untrustworthy, ultimately impacting the organisation's reputation and bottom line.

6.3 Challenges organisations face in complying with the Nigeria Data Protection Legislation

The participants in this study offered valuable insights into the challenges they face in complying with data protection legislation. Regulators must pay close attention to these issues and work towards practical solutions to address them effectively.

The primary challenges highlighted regarding privacy compliance in Nigeria include:

1. **Lack of Awareness and Understanding:**

a. Many organisations, particularly those without dedicated Data Protection Officers (DPOs), struggle with limited awareness and understanding of the Nigeria Data Protection Act (NDPA) 2023.

2. **Lack of Sector-Specific Guidelines:**

a. The Nigeria Data Protection Commission (NDPC) does not provide industry-specific guidelines or practical templates, making compliance efforts more complex.

3. **Unclear Requirements:**

a. Some provisions of the NDPA are perceived as vague, making it difficult for organisations to understand and implement them effectively.

4. **Internal Resistance to Compliance:**

a. Businesses face challenges in getting other departments to prioritise and adhere to data protection measures.

5. **Perceived Lack of Importance:**

a. Data protection is often viewed as a low priority, further delaying compliance efforts.

6. **Subjective Interpretation:**

a. Certain directives are seen as open to subjective interpretation, creating inconsistency in implementation.

7. **Weak Enforcement:**

a. The lack of strong enforcement of data protection laws diminishes their perceived importance, reducing compliance incentives.

8. **Resource and Cost Challenges:**

a. Compliance with the NDPA can be financially and resource-intensive, posing significant challenges, particularly for small and medium-sized enterprises (SMEs).

6.4 'Has the guidance provided by NDPC been useful in understanding your responsibilities as a Data Controller/Processor?'

The survey results indicate varying levels of satisfaction with the guidance provided by the data protection commission regarding roles as a controller or processor:

- 44% of the overall respondents found the guidance provided by the commission useful in understanding their roles, indicating that a significant portion of organisations has benefited from the guidance.
- 26% of the overall respondents did not find the guidance useful, suggesting that these individuals may have encountered difficulties in applying or interpreting the information provided.
- 30% of the overall respondents were unsure about the usefulness of the guidance, which could imply that they have not had the opportunity to read or are unaware of the existence of such guidance.

The survey results, broken down by sector, show the following insights regarding the usefulness of the guidance provided by the data protection commission:

Private Sector:

50%

of the respondents found the guidance useful in understanding their roles as a controller or processor.

23%

of the respondents did not find the guidance useful.

27%

of the respondents were unsure whether the guidance was useful, possibly indicating a lack of awareness or engagement with the guidance.

Public Sector:

40%

of the respondents found the guidance useful, like the private sector.

20%

of the respondents did not find the guidance useful.

40%

of the respondents were unsure whether the guidance was useful to them, suggesting a lack of clarity or awareness, or understanding regarding the application of the guidance.

These results point to a need for the commission to improve the clarity, accessibility, or communication of its guidance to better support organisations in complying with data protection legislation.

The feedback indicates a general dissatisfaction with the current efforts made by the commission to aid compliance, highlighting a gap in effectiveness that may require attention. By addressing these barriers, regulators can promote a culture of compliance, simplify processes, and ensure that organisations of all sizes can effectively meet data protection requirements. This could include introducing sector-specific guidelines, enhancing enforcement, providing educational resources, and supporting SMEs with scalable solutions.

Section 7: Conclusion

The findings of this report show the critical need for stronger data protection compliance frameworks across Nigerian organizations. While some organisations demonstrate proactive efforts in implementing privacy policies, conducting DPIAs, and integrating privacy into enterprise risk management, significant gaps remain, particularly in training, awareness, third-party risk management, and regulatory enforcement.

The lack of universal compliance with key requirements, such as responding to Subject Access Requests (SARs), appointing Data Protection Compliance Organizations (DPCOs), and filing compliance audit returns, highlights the need for more structured regulatory oversight. Furthermore, the emerging challenges posed by AI, emerging technologies, and insider threats emphasize the importance of continuous adaptation and strategic privacy risk management.

To strengthen compliance, organizations must prioritize robust governance, invest in employee training, and leverage automation tools for privacy risk management. Regulators, on the other hand, should enhance sector-specific guidance, enforce compliance more strictly, and support SMEs with practical, scalable solutions.

Ultimately, fostering a culture of data protection will require a collective effort from businesses, regulators, and consumers. By addressing the gaps identified in this report, Nigerian organizations can build greater trust in data privacy, mitigate security risks, and align with global best practices in data protection compliance.

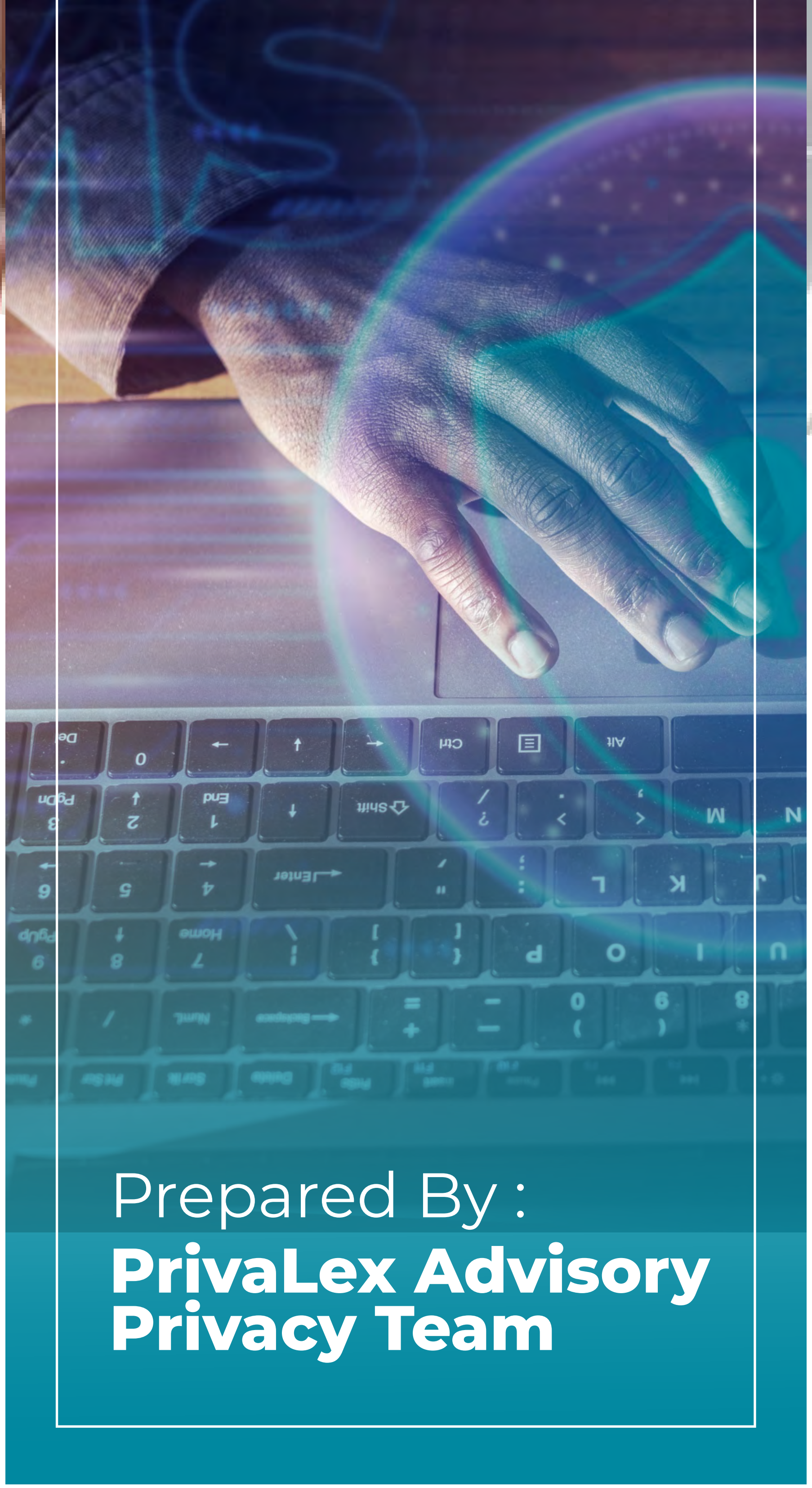
PrivaLex Advisory
...Compliance Redefined, Privacy Secured

UK Office: Suite 5058, Unit 3A, 34-35 Hatton Garden, Holborn, London ECIN 8DX
Nigerian Office: Block E, New Providence Garden, Opposite Russel International School, Lekki, Lagos.

☎ **Landline:** +234 (0) 813 358 6403 -Nigeria
+44 (0) 3030401065 -London

Website: www.privalexadvisory.com

✉ **E-mail:** contact@privalexadvisory.com



Prepared By :
PrivaLex Advisory Privacy Team