Published by

Nigeria Data Protection Commission (NDPC)

Facebook: @ndpcngr

Twitter: @ndpcngr

Instagram: @ndpcnigeria

LinkedIn: Nigeria Data Protection Commission - NDPC

YouTube: Nigeria Data Protection Commission

Website: www.ndpc.gov.ng

©Nigeria Data Protection Commission

2nd Edition, 2026

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means electronic, mechanical, photocopying, recording, or otherwise without the prior permission of the Nigeria Data Protection Commission, Abuja, the copyright owner.

Printed and bound in Nigeria by Amatt Brill Impressions Ltd.

Block A2, Suite & Commerce Plaza,

Garki, Abuja.

Editorial Note

It is with great pleasure that we present the Second Edition of the *NDPC - International Journal of Data Privacy and Protection*, themed **"Advancing Compliance and Safeguarding Rights in the Age of Emerging Technologies".** This edition builds on the foundation laid by our inaugural publication and reflects the growing maturity, urgency, and relevance of data protection discourse within Nigeria and across the global digital ecosystem.

The rapid evolution of emerging technologies—such as Artificial Intelligence, Big Data Analytics, Biometric Systems, Blockchain, and the Internet of Things continues to redefine how personal data is collected, processed, shared, and governed. While these technologies offer unprecedented opportunities for innovation, economic growth, and improved service delivery, they also pose complex challenges for regulatory compliance, accountability, and the protection of fundamental rights – particularly the right to privacy. This edition responds directly to these realities by interrogating how legal, institutional, and technical frameworks can remain effective, adaptive, and rights-centred in an era of constant technological change.

The articles featured in this volume provide rich, multidisciplinary perspectives on contemporary data protection issues. Contributors examine practical compliance strategies under evolving regulatory regimes, emerging risks to privacy and data subject rights, the role of regulators, data controllers, processors, and other stakeholders in fostering a culture of responsible data governance. Of particular importance is the emphasis on safeguarding individual rights, fairness, transparency, accountability, and redress, while enabling innovation and digital transformation.

This Journal serves as a platform for rigorous scholarship, policy-relevant analysis, and knowledge exchange among regulators, academics, practitioners, industry players, and civil society. It is our conviction that evidence-based research and informed dialogue are critical to strengthening compliance, deepening public trust, and advancing a just and inclusive digital economy.

We extend our sincere appreciation to all authors, peer reviewers, editorial advisers and members of the editorial team whose dedication and intellectual contributions have made this edition possible. We also acknowledge our readers for their continued engagement and commitment to advancing data privacy and protection.

As emerging technologies continue to reshape our societies, we hope this edition will stimulate critical reflection, guide policy and practice, and contribute meaningfully to the collective effort to protect personal data and uphold human dignity in the digital age.

Dr. Vincent Olatunji, *CDPO, CPPPS, FIIM*
National Commissioner/CEO
Nigeria Data Protection Commission (NDPC)

Editor in Chief

Dr. Vincent Olatunji, *CDPO, CPPPS, FIIM*

Editor

Tolulope Pius-Fadipe, *PhD, CDPO, CPM*

Editorial Advisers

Babatunde Bamigboye, *Esq., LLB, BL, LLM, CDPRP*

Tokunbo Smith, *CDPSE, FIIM, FITD, FIMC, FOSHA (UK)*

Editorial Team

Olayinka Oyebanji, *CDPO*

Saratu Samande, *Esq., CDPO*

Ibukunoluwa Owa, *Esq., CIPP/E*

Seyi Dare-Davids, *CDPO*

Alexander Onwe, *Esq., CDPO*

Abdulmalik Jamoh, *CDPO*

Abubakar Bello, *CDPO*

Kayode Odekunle, *CDPO*

Table of Contents

Editorial Note iii

The General Application and Implementation Directive (GAID): Operationalising the Nigeria Data Protection Act, 2023 1

Naming, Nudging, and Navigating Compliance: Comparative Lessons in Data Protection Enforcement from Nigeria and Canada 10

Regulatory Compliance: Best Practices, Challenges and Enforcement under the Nigeria Data Protection Act (NDP Act), and Global Frameworks (GDPR, etc.) 20

Regulating Children's Interactions with AI: Privacy, Safety, and Social Impact 33

Procurement as a Privacy Lever: Embedding Privacy by Design in Government Contracts and Vendor Selection 43

From Fragmentation to Integration: Nigeria's Role in Pan-African Data Governance and Privacy Harmonisation 53

The New Currency is Compliance: Navigating Data Protection in a Borderless Digital Economy 66

From CI/CD (Continuous Integration / Continuous Deployment) to CI/CDP (Continuous Integration / Continuous Data Protection): Embedding Privacy by Design in DevOps Workflows for Scalable Compliance 76

Data Subject Rights in Nigeria: Bridging the Gap Between Policy and Practice 86

The Efficacy of Privacy Self-Management in the Era of Artificial Intelligence 100

Building a culture of Data Protection: A Pedagogical Basis for Data Privacy Literacy in Nigerian Universities 111

Data Subject Rights: Real World Application of Rights to Access, Rectification, Object, Erasure, and Data Portability 121

Privacy by Design and Default: Integrating Privacy Principles into Systems, Services, AI Models and Digital Infrastructure 131

Data Privacy and the Legal Practice: Ensuring Compliance in Nigeria's Emerging Tech Landscape 141

Emerging Technologies and the Future of Data Protection in Nigeria: Safeguarding Rights in the Age of AI, Surveillance, and Digital Sovereignty 151

Predictive Analytics, AI, and the Future of Data Protection: Risks, Rights, and Regulatory Imperatives 160

Data Sovereignty in Africa: Balancing National Interests and Global Data Flows 169

Strengthening Proactive Data Protection through DPIAs and Risk-Based Approaches 180

Balancing Innovation and Privacy: Advancing Data Protection and Governance in Nigeria's Digital Economy 190

The General Application and Implementation Directive (GAID): Operationalising the Nigeria Data Protection Act, 2023

Dr Vincent Olatunji, CDPO, CPPPS, FIIM
National Commissioner/CEO,
Nigeria Data Protection Commission (NDPC)
nc@ndpc.gov.ng

ABSTRACT

The enactment of the Nigeria Data Protection Act (NDP Act), 2023 marked a decisive milestone in Nigeria's digital governance trajectory, establishing a comprehensive legal framework for the protection of personal data and the promotion of trust in the digital economy. While the Act provides the legal foundation for data protection in Nigeria, its effectiveness ultimately depends on clear, consistent, and practical implementation across both public and private sectors. Consequently, the General Application and Implementation Directive (GAID), issued by the Nigeria Data Protection Commission (NDPC) on 20th March 2025 with an effective date of 19th September 2025, serves as the operational blueprint for the NDP Act, providing much-needed clarity and practical guidance on the application of the Act. The GAID is not merely a supplementary instrument but is the regulatory mechanism through which the objectives of the NDP Act are translated into actionable compliance obligations. It provides clarity on the scope of the Act, standardises compliance expectations, and prescribes procedures relating to registration, compliance audit returns, accountability measures, enforcement, and cross-border data transfers. In doing so, the GAID aims to promote regulatory certainty, risk-based oversight, and responsible data governance within Nigeria's rapidly evolving digital ecosystem. This paper provides an overview of the GAID, explores its key provisions, and assesses its practical implications for data controllers, processors, regulators, and data subjects. The paper further evaluates the GAID's significance as a governance tool for enhancing compliance, strengthening institutional oversight, and fostering trust in the digital economy.

Keywords: Nigeria Data Protection Act, Data Protection Compliance, Personal Data, Data Governance, GAID

1. Introduction

Nigeria's data protection regime experienced a crucial turning point with the enactment of the NDP Act, 2023. Prior to this, data governance relied principally on the Nigeria Data Protection Regulation (NDPR) 2019 and accompanying frameworks, which, while significant, lacked the

statutory force and comprehensive reach of an act of parliament. Recognising the limitations of the NDPR and the growing imperative for an enforceable data protection law, the Nigerian government passed the NDP Bill, 2023 into law to strengthen data protection in the country.[1]

The NDP Act, 2023 establishes the Nigeria Data Protection Commission (NDPC) as the principal regulator, prescribes enforceable data rights, and imposes obligations on data controllers and processors concerning the processing of personal data.[2] It also aligns Nigeria with global data protection standards, notably the General Data Protection Regulation (GDPR) of the European Union, thereby facilitating international data flows and strengthening cross-border commercial trust.

Like many modern, principles-based data protection laws, the NDP Act is designed to establish foundational rights, obligations, and institutional mandates, while envisaging further regulatory instruments to guide detailed implementation. Accordingly, the issuance of the General Application and Implementation Directive (GAID) represents a deliberate and necessary step in giving practical effect to the legislative intent of the NDP Act, 2023. The NDPC issued the GAID to clarify the application of the Act's provisions, provide guidance, and ensure consistency, proportionality, and legal certainty in enforcement. Rather than replacing the Act, the GAID functions as its operational blueprint, translating legislative principles into actionable obligations and enabling the NDP Act to function as a living regulatory framework responsive to Nigeria's dynamic digital economy.[3]

The development of the GAID was characterised by extensive stakeholder engagement, reflecting the NDPC's commitment to regulatory inclusiveness. Consultations involved representatives from industry, civil society, legal practitioners, technological experts, and data subjects themselves, ensuring that the GAID was informed by real-world complexities and sectoral nuances. This participatory approach not only enhanced the legitimacy and acceptability of the GAID but also contributed to its operational adaptability.[4]

2. Key Elements of the GAID

2.1 Scope

One of the most significant clarifications provided by the GAID is the extraterritorial application of the Nigeria Data Protection Act. The Directive affirms that the Act applies not only to entities established in Nigeria, but also to entities that lack a physical presence in the country where their processing activities have a sufficient nexus to Nigeria or to data subjects connected to Nigeria. Accordingly, an entity will fall within the scope of the Act where it processes personal data relating to a data subject in Nigeria, or targets the personal data of data subjects in Nigeria; where the data subject is physically present within the territory of Nigeria, irrespective of nationality or migration status; where personal data has been transferred to Nigeria; where personal data is in transit

[1] Ahmed, H & Muhammad, S, *"Assessing the Adoption of Nigeria Data Protection Act (2023): A Case Study of Some Selected Higher Institutions in North-Eastern Nigeria* (Open Journal of Physical Science), 14.
[2] Nigeria Data Protection Act, No. 3 of 2023 (Nigeria).
[3] Nigeria Data Protection Commission (NDPC), *Nigeria Data Protection Act – General Application and Implementation Directive (GAID)*, issued March 20, 2025.
[4] KPMG Nigeria, Review of the NDPA General Application and Implementation Directive (GAID) 2025 (Lagos: KPMG Nigeria, May 2025).

through Nigeria; or where the processing relates to a Nigerian citizen who is not physically present in Nigeria.

Importantly, the GAID provides that where there is any inconsistency between the NDP Act and the GAID, the provisions of the Act prevail. This ensures that the GAID operates as an administrative instrument subordinate to the statute.

2.2 Overarching Principles

The GAID reaffirms the foundational principles of data protection enshrined in the NDP Act, 2023 including lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability.

2.3 Lawful Bases for Processing and Provisions for Reliance

The GAID affirms the lawful bases for the processing of personal data as established under the NDP Act, 2023 and provides practical guidance on reliance on these bases in operational contexts. By articulating conditions for reliance on each lawful basis, the GAID assists data controllers and processors in determining the appropriate legal justification for specific processing activities and in documenting such reliance for compliance and supervisory purposes. This clarification enhances legal certainty, supports accountability, and facilitates consistent regulatory interpretation and enforcement under the NDP Act.

The GAID further identifies circumstances in which consent is required as the lawful basis for processing[5]. These include processing for direct marketing purposes, the processing of sensitive personal data, processing that is incompatible with the original purpose of collection, the processing of children's personal data, the transfer of personal data to countries for which the regulator has not issued an adequacy decision, and decisions based solely on automated processing that produce legal or similarly significant effects on the data subject. By clarifying these consent-dependent contexts, the GAID reinforces the centrality of informed and freely given consent in high-risk processing activities and provides greater certainty for controllers in selecting and documenting an appropriate lawful basis under the Act.

2.4 Data Subject Rights and Exercise Procedures

The GAID elaborates on the mechanisms for enabling data subject rights under the NDP Act. It prescribes standardised forms for rights requests, timelines for responses, and procedures for verifying the identity of requesters. The GAID also sets out clear requirements for privacy notices and cookie disclosures to strengthen meaningful transparency. In addition, the GAID requires data controllers to maintain records of all data subject requests and corresponding responses.

Furthermore, the GAID also provides guidance on balancing the rights of data subjects against legitimate interests or legal obligations of data controllers, offering illustrative scenarios and risk-based assessment criteria. For instance, in cases where data erasure may conflict with statutory record-keeping duties, the GAID outlines a proportionality test and mandates documentation of the decision-making process.

---

[5] See GAID - Article 17

2.5 Registration and Classification of Data Controllers and Processors[6]

The GAID introduces a tiered approach to registration and supervisory oversight. Data Controllers and Processors are classified into categories based on factors such as volume of personal data processed, the sensitivity of the data, and the potential impact of processing on data subjects. The categories are as follows:

i. **Ultra-High Level (UHL):** Entities, who, among others, process personal data of over 5,000 data subjects, and are expected to abide by global and highest attainable data protection standards. Such entities are required to pay a registration fee of ₦250,000 and an additional data processing activities fee of ₦5,000 for each processor engaged.
ii. **Extra-High Level (EHL):** Entities, who, among others, process personal data of over 1,000 data subjects and are expected to abide by global best practices of data protection, with a registration fee of ₦100,000.
iii. **Ordinary-High Level (OHL):** Entities who, among others, process personal data of over 200 data subjects and are also required to comply with global best practices, with a registration fee of ₦10,000.

Data Controllers/Processors in UHL and EHL categories are required to register once with the NDPC, but must file Compliance Audit Returns (CAR) with the NDPC annually, while OHL category must renew their registration annually, but are not required to file CAR with the NDPC.

2.6 Appointment and Role of Data Protection Officers (DPOs)

The GAID reaffirms the appointment of DPOs as enshrined in Section 32 of the NDP Act and provides detailed guidance on the role, independence, reporting lines, and conflict-of-interest safeguards applicable to DPOs, ensuring that they can perform their functions effectively and without undue influence. In doing so, GAID reinforces the DPO's position as a central accountability mechanism within organisational data protection governance frameworks. To enable the effective discharge of these responsibilities, the GAID requires that DPOs have unrestricted access to personal data and processing activities relevant to their functions, while also imposing an obligation of confidentiality in respect of information obtained in the course of their duties.

The GAID further establishes a central registry of DPOs to be maintained by the NDPC and requires organisations to notify the Commission of all DPO appointments. Data controllers are also required to make the contact details of their DPOs publicly available, thereby enhancing transparency and accessibility for data subjects. In addition, the GAID mandates structured internal accountability by requiring DPOs to submit semi-annual reports to organisational management on the state of data protection compliance. To ensure sustained professional competence, the Directive empowers the NDPC to conduct periodic credential assessments of DPOs and encourages continuous capacity-building and professional development, reflecting the evolving and technical nature of data protection compliance.

[6] See GAID - Article 9 & Schedule 7

2.7 Data Privacy Impact Assessments (DPIAs)[7]

Recognising the central role of risk assessment in effective data protection, as such, the GAID mandates the conduct of DPIAs for processing activities that are likely to result in high risks to the rights and freedoms of data subjects. It sets out the core elements of a DPIA, including a description of the envisaged processing operations, an assessment of their necessity and proportionality, the identification of potential risks to data subjects, and the measures envisaged to address and mitigate those risks. To support consistent application, Schedule 4 of the GAID introduces a standardised DPIA template and specifies threshold criteria for determining when a DPIA is required, thereby reducing uncertainty and encouraging proactive risk management by data controllers.

2.8 Standard Notice to Address Grievance (SNAG)[8]

Schedule 9 of the GAID introduces the data subject's SNAG as a mechanism for the resolution of data protection complaints. The SNAG provides a standardised format through which a data subject may notify a data controller or processor of an alleged violation of the NDP Act and request remedial action before escalating the matter to the NDPC. By formalising this pre-complaint engagement process, the GAID encourages timely internal resolution of grievances, promotes accountability, and reduces unnecessary regulatory escalation, while preserving the data subject's right to seek regulatory intervention where grievances remain unresolved.

2.9 Data Breach Notification and Response[9]

In operationalising the NDP Act's breach notification requirements, the GAID prescribes procedures for breach detection, risk assessment, notification to the NDPC within 72 hours of discovery, and communication to affected data subjects where there is a high risk to their rights. It also specifies the required content of breach notifications, including the nature of the breach, categories of data affected, likely consequences, and remedial measures taken. To promote preparedness, the GAID requires data controllers to maintain incident response plans, breach registers, and staff training programmes, and clarifies the NDPC's investigative and cooperation powers in cases involving cross-border or multi-jurisdictional breaches.

2.10 Cross-Border Data Transfers and Cross-Border Processing[10]

The GAID provides guidelines as to the relevant factors to consider for data transfer such as adequacy decisions by the NDPC, approved cross-border transfer instruments (CBTIs), and other lawful bases, subject to specified safeguards. The Directive requires controllers to document transfer mechanisms and to ensure that foreign recipients provide protections comparable to those required under the NDP Act. This framework is aligned with international practices and gives NDPC the discretion to adopt adequacy determinations and to approve model contractual clauses or other transfer instruments.

---

[7] See GAID - Article 28 & Schedule 4
[8] See GAID - Article 45 & Schedule 5
[9] See GAID - Article 33
[10] See GAID - Article 45 & Schedule 5

2.11 Emerging Technologies[11]

The GAID imposes specific compliance obligations on organisations seeking to deploy emerging technologies that involve personal data processing. Such organisations are required to implement appropriate technical and organisational measures and to give due consideration to the data subject's right not to be subjected to decisions based solely on automated processing or algorithmic systems. The Directive further requires the conduct of Data Protection Impact Assessments prior to deployment, as well as the testing of emerging technologies in low-risk or controlled environments. In addition, organisations must evaluate the likelihood of disparate, biased, or unintended outcomes arising from such technologies and assess whether such risks can be effectively mitigated. To ensure ongoing compliance, the GAID emphasises the need for continuous monitoring and periodic re-testing of emerging technologies in order to identify and reduce evolving privacy risks.

2.12 Enforcement, Sanctions, and Remedies

The GAID clarifies the NDPC's enforcement powers, procedures for investigation, administrative fines, and remedial orders. It sets out factors to be considered in determining sanctions, including the nature and gravity of the breach, the number of data subjects affected, intent or negligence, and prior compliance history. The GAID also provides guidance on cooperation with other regulatory agencies, dispute resolution, and avenues for data subjects to seek redress.[12]

3.0 Assessment of the GAID's Effectiveness

3.1 Enhancing Legal Certainty and Predictability

By translating the broad principles of the NDP Act, 2023 into actionable compliance requirements, the GAID reduces ambiguity and promotes consistency in interpretation and application across sectors. This is particularly important in a jurisdiction such as Nigeria, where a diverse range of actors, sectors, and technological contexts could otherwise result in fragmented and uneven compliance practices. Through standardised procedures, templates, and timelines, the GAID lowers barriers to compliance and supports the development of a culture of accountability and regulatory adherence across the data protection ecosystem.

3.2 Balancing Flexibility and Regulatory Rigour

A key challenge in operationalising laws is navigating the delicate balance between regulatory flexibility to encourage innovation and regulatory rigidity to ensure enforceability and prevent loopholes.[13] The GAID balances this by adopting risk-based approaches throughout its provisions. It differentiates between high and low-risk processing activities and delineates compliance obligations accordingly. At the same time, the Directive avoids the pitfalls of over-generalisation by setting clear minimum standards and non-negotiable requirements. This hybrid approach enhances both the effectiveness and adaptability of the regulatory regime.

---

[11] See GAID - Articles 43 & 44

[13] Josh Sannu and Golry Maxwell, "Balancing Innovation and Compliance: The Role of Regulators in Digital Finance Ecosystems," November 2024.

3.3 Promoting Accountability and Transparency

The GAID's operational guidance is underpinned by a strong emphasis on accountability and transparency. By requiring data controllers and processors to document their compliance efforts, it institutionalises a culture of proactive risk management and demonstrable compliance. This not only facilitates regulatory oversight but also empowers data subjects by providing clearer avenues for exercising their rights.

3.4 Capacity Building and Ecosystem Growth

The GAID goes beyond rule-setting by promoting capacity building and continuous regulatory dialogue through training for Data Protection Officers and staff, the development of professional standards, and structured stakeholder engagement. These measures strengthen institutional competence while also supporting the growth of Nigeria's data protection ecosystem by creating demand for skilled professionals and compliance services across various sectors, thereby contributing to the sustainable expansion of the digital economy.

4.0 Implications for Stakeholders

4.1 For Data Subjects

The GAID's operationalisation of data subject rights, transparency obligations, and remedies represents a significant advance in informational self-determination. By clarifying procedures and timelines for rights requests, mandating breach notifications, and facilitating redress, the Directive empowers data subjects and enhances their ability to hold organisations accountable.

4.2 Data Controllers and Processors

The GAID provides both opportunities and obligations for data controllers and processors. On the one hand, it provides much-needed clarity and predictability, reducing legal uncertainty and facilitating compliance; on the other hand, it elevates the standard of care in data processing, requiring investments in systems, processes, human capital development, and documentation.
Organisations that proactively comply with the GAID will derive competitive advantages, including enhanced trust from customers and partners, reduced risk of sanctions, and improved operational resilience.[14]

4.3 The Broader Digital Economy

At a macro level, the GAID's contribution to regulatory certainty, stronger data governance, and enhanced digital trust has positive implications for Nigeria's digital economy. By aligning with international standards and facilitating lawful cross-border data flows, the GAID improves Nigeria's attractiveness for investment, innovation, and international partnerships. It also strengthens Nigeria's position as a regional leader in data protection regulation, supporting broader efforts toward regulatory harmonisation and digital integration across Africa.

---

[14] G. Elias & Co., *Highlights of the Nigeria Data Protection Act General Application and Implementation Directive, 2025*.

5.0 Comparative Perspectives and International Alignment: Lessons from International Practice

The issuance of the GAID is consistent with international regulatory practice, where data protection authorities adopt secondary instruments, guidelines, and directives to operationalise statutory data protection frameworks and provide clarity on compliance obligations. A similar approach is the European Union's General Data Protection Regulation (GDPR) Articles and Recitals, which provides extensive regulatory guidance.[15] By adopting this model, the GAID aligns Nigeria's data protection regime with global governance trends while reflecting Nigeria's national context.[16]

6.0 Implementation Roadmap: Practical Guidance for Stakeholders

6.1 Data Subjects

The GAID strengthens avenues for exercising statutory rights under the NDP Act, including the rights of access, rectification, erasure, objection, and complaint. To benefit from these protections, individuals are encouraged to actively engage available mechanisms by submitting rights requests through prescribed formats and making use of standard grievance procedures where violations are suspected. Data subjects are also encouraged to exercise caution and informed judgment when providing personal data, particularly in digital and commercial contexts, and to review privacy notices and consent requests before engaging with services. Where internal complaint mechanisms fail to resolve grievances, the matter may be escalated to the NDPC.

6.2 Data Controllers and Processors

For data controllers and processors, compliance with the GAID requires a shift from ad hoc compliance measures to structured and sustained data governance practices. Organisations should begin with comprehensive gap assessments to map existing processes against GAID requirements, including registration obligations, lawful basis documentation, data subject rights procedures, breach response mechanisms, and the need for DPIA. High-risk processing activities, particularly those involving large-scale or sensitive data, should be prioritised for immediate risk assessment and mitigation.

Embedding privacy by design and by default into operational workflows, procurement processes, and system development lifecycles will be critical to long-term compliance. Organisations should also put in place internal accountability mechanisms, including empowered Data Protection Officers, and staff training programmes. For entities engaged in cross-border data transfers, regular review of contractual safeguards and transfer mechanisms will be necessary to meet evolving regulatory expectations under the GAID, maintaining international trust and interoperability.

6.3 The Regulator (NDPC)

The effective implementation of the GAID will depend on sustained investment in institutional capacity, supervisory tools, and inter-agency coordination. Priority would be given to

---

[15] European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), Official Journal of the European Union L119 (2016)

[16] Banwo & Ighodalo, "Synoptic Analysis of the Nigeria Data Protection Act – General Application and Implementation Directive (GAID) 2025," April 30, 2025.

strengthening technical expertise and expanding regional supervisory presence to support proactive and risk-based enforcement. Given the cross-cutting nature of data processing activities, continued collaboration with sectoral regulators and public institutions will be essential to ensure regulatory coherence and to prevent overlapping or inconsistent compliance expectations.[17]

The Commission will also issue sector-specific guidelines and compliance toolkits that will support regulated entities in understanding evolving expectations, particularly in high-risk or emerging technology contexts. Continuous stakeholder engagement and periodic review of implementation challenges will further enable the NDPC to refine regulatory strategies while maintaining public confidence in the enforcement process.

7.0 Conclusion

As Nigeria navigates the complexities of the digital age, the GAID stands as a blueprint, translating statutory obligations of the Nigeria Data Protection Act, 2023 into practicable regulatory measures that will shape Nigeria's data protection landscape and position the country at the forefront of African digital governance.

The GAID's success will depend on implementation, both by regulated entities who must embed privacy into daily operations and by the NDPC, which must marshal the capacity, clarity, and proportionality needed for credible enforcement. By sharpening inter-regulatory collaboration and adopting proportionate, capacity-aware enforcement, Nigeria can ensure the GAID delivers on the NDP Act's core objective of safeguarding the rights of data subjects while enabling Nigeria's full participation in regional and global economies through trusted and beneficial use of personal data.

Naming, Nudging, and Navigating Compliance: Comparative Lessons in Data Protection Enforcement from Nigeria and Canada

Jadesola Olasubulumi, PhD
Bank of Montreal (BMO) Toronto, Canada
jadesolaolasubulumi@gmail.com.

ABSTRACT

This paper offers a critical comparative analysis of regulatory enforcement under Nigeria's *Data Protection Act* (NDP Act) and Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA), focusing on how their respective data protection authorities- the Nigeria Data Protection Commission (NDPC) and Office of the Privacy Commissioner of Canada (OPC) shape compliance behaviour across sectors. It highlights divergent enforcement cultures: Nigeria's assertive reliance on sanctions and public exposure of non-compliant entities, versus Canada's cooperative model built on guidance, voluntary compliance, and reputational pressure. Drawing on enforcement actions including NDPC's sanctioning of MultiChoice Nigeria and publication of over 1,000 non-filing organisations, as well as OPC's investigations into Facebook, Equifax, and sector-wide breach-reporting, the paper interrogates whether visible deterrence fosters meaningful accountability or risks procedural overreach, and whether cooperative approaches build trust at the expense of deterrence. It argues for a hybrid model that integrates sanctions with fairness, transparency with due process, and cooperation with credible deterrence. Policy recommendations are tailored to each jurisdiction while advancing reforms applicable to both. By centring enforcement practice and situating it within global governance debates, the paper contributes a comparative framework for evaluating hybrid enforcement models in data protection.

Keywords: Data Protection Enforcement, Data Protection Authority, Sanctions and Deterrence, Compliance Culture, Comparative Privacy Law, Institutional Trust

1. Introduction

The effectiveness of data protection laws depends not only on the quality of the legal text but also on the ability of regulators to translate those rules into lived compliance. In this regard, the enforcement strategy of a Data Protection Authority serves as both a mirror and a mold- it reflects the state of regulatory maturity and shapes the compliance culture that evolves around it. While most jurisdictions converge on core principles such as lawful processing, accountability, and data subject rights, their enforcement practices diverge sharply in tone and tools. This paper examines two illustrative regimes: Nigeria's NDP Act (2023), enforced by the NDPC and Canada's PIPEDA (2001) overseen by the OPC. Both share commitments to

privacy protection but adopt distinct enforcement postures: Nigeria leads with visibility and sanctions, while Canada privileges persuasion and guidance. These contrasts are not merely stylistic but structural, rooted in statutory design, institutional capacity, and regulatory philosophy.

By analysing emblematic enforcement cases and situating them within broader theoretical debates, this paper explores how regulators influence compliance, credibility, and public trust in digital economies. The aim is not to valorise one model over the other but to distill lessons for constructing context-sensitive and sustainable enforcement frameworks.

2. Contextual Foundations: Legal and Institutional Landscapes

2.1. The NDP Act and the NDPC

Enacted in June 2023, the *NDP Act*[18] marked a pivotal development in Nigeria's digital governance landscape. It established a comprehensive regime for the collection, processing, and protection of personal data and created the NDPC replacing the Nigeria Data Protection Bureau (NPDB) as an independent supervisory authority with broad investigatory and enforcement powers.[19]

Section 5 of the NDP Act outlines the Commission's statutory functions, including investigating complaints, issuing compliance directives, promoting awareness, and advising government. Section 46 further empowers data subjects to petition the NDPC directly, empowering it to investigate alleged violations. Complementing these provisions, Section 48 enables the issuance of binding enforcement orders, imposition of penalty or remedial fines, thereby equipping the Commission with both preventive and corrective tools to safeguard personal data. The Act establishes a structured enforcement pathway. Investigations may begin with a complaint lodged by a data subject or be initiated *suo motu* where a breach or likely breach is suspected.[20] The NDPC can compel oral testimony, require production of documents, and demand sworn statements. Where violations are confirmed, compliance orders may direct remedial steps, grant grace periods, and in some cases compel controllers to facilitate rights under Section 34, such as the right to erasure. Importantly, such orders remain subject to judicial review within thirty days, embedding procedural safeguards within the enforcement framework.

A key innovation of the NDP Act lies in its two-tier system of administrative fines.[21] Controllers or processors of "major importance" may face penalties of up to the greater of ₦10 million or 2% of annual gross revenue, while smaller entities may be fined up to ₦2 million or 2% of revenue. In setting the scale of fines, the NDPC must consider factors including the seriousness, duration, and intent of the infringement, the nature of the compromised data, and the offender's level of cooperation. This calibrated model seeks to align sanctions with the gravity of misconduct, combining deterrent, corrective, and preventive elements while preserving access to judicial oversight.

---

[18] Federal Republic of Nigeria, *Nigeria Data Protection Act, 2023* (Abuja: Federal Government of Nigeria), https://cert.gov.ng/ngcert/resources/Nigeria_Data_Protection_Act_2023.pdf
[19] Olumide Babalola and Paolo Balboni, *Annotated Nigeria Data Protection Act*, 2023 (Noetico Repertun Inc, 2024).
[20] Ikenga Oraegbunam and Tega Edema, "The Legal regime for Data Protection in Nigeria: The Nigeria Data Protection Commission in Focus," *International Review of law and Jurisprudence* 5, no. 3 (2023): 128-133.
[21] Olumide Babalola, "The GDPR-Styled Nigeria Data Protection Act 2023 and the Reverberations of a Legal Transplant" *British Journal of Cyber Criminology* 3, no.1 (2024):106-110.

Beyond administrative penalties, the NDP Act also embeds escalation to criminal sanctions in cases of persistent or willful non-compliance. Section 48(1) clarifies that regulatory enforcement does not preclude criminal sanctions, while Section 49(1) stipulates that failure to comply with a compliance order constitutes an offence. Upon conviction, defaulting entities may face fines at either the higher or standard maximum levels, imprisonment of up to one year, or both. The integration of criminal sanctions alongside administrative remedies underscores the NDPC's authority, signaling that remediation is prioritised, but coercive escalation remains available for persistent defiance.

Since its establishment, the NDPC has acted swiftly to operationalise its mandate. It has issued implementation frameworks such as the General Application and Implementation Directive (GAID),[22] accredited more than 300 DPCOs, and launched sector-wide audits. In 2024, it reported 213 active investigations across key sectors and audited more than 2,000 companies.[23] In 2025, it fined Multichoice Nigeria ₦766,242,500 for privacy violations involving cross-border data transfers[24] and published a list of over 1,000 non-compliant organisations spanning finance, insurance, and gaming.[25] These measures illustrate an assertive enforcement culture where visibility and reputational pressure are integral tools.

Taken together, the NDP Act equips the NDPC with a layered and coercive framework that blends investigatory powers, compliance orders, administrative fines, and potential criminal liability. In both design and execution, Nigeria's regime aligns more closely with the sanction-oriented traditions of European data protection authorities than with Canada's more conciliatory enforcement model under PIPEDA

2.2. PIPEDA and the OPC

Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA) came into force in 2001.[26] It was introduced to build consumer trust in e-commerce, enhance competitiveness in the digital economy, and usher in a new era of privacy protection in Canada.[27] The Act establishes rules governing how private-sector organisations collect, use, and disclose personal information in the course of commercial activities. Oversight is entrusted to OPC, which also enforces the *Privacy Act* applicable to federal institutions.

The OPC's mandate under PIPEDA includes investigating privacy complaints and providing organisations with guidance to strengthen their information-handling practices.[28] Originally established as an alternative to costly litigation under the *Privacy Act*, the OPC follows an

---

[22] Adewumi Salami and Caleb Nmeribe "Nigeria: NDPC Issues GAID- Key Compliance Insights." *DLA Piper*, June 3, 2025, https://privacymatters.dlapiper.com/2025/06/nigeria-ndpc-issues-gaid-key-compliance-insights/

[23] Nigeria Data Protection Commission, *Nigeria Data Protection Annual Report 2024*.

[24] Nigeria Data Protection Commission, "Press Release: NDPC Fines Multichoice Nigeria #766, 242,500 for Violating NDP Act," July 6, 2025, https://ndpc.gov.ng/category/news/.

[25] "NDPC Cracks down on 1, 369 Nigerian Firms over Data Privacy Violations," *Techpoint Africa*, August 25, 2025. https://techpoint.africa/news/ndpc-targets-1369-companies/

[26] Department of Justice Canada. *Personal information Protection and Electronic Documents Act.* https://laws-lois.justice.gc.ca/pdf/p-8.6.pdf

[27] Imran Barbacki and Katherine Barbacki, "Recent Developments in Canadian Privacy Law and the Digital Charter." *The Business lawyer* 75 (2019-2020): 1647-1654.

[28] Office of the Privacy Commissioner of Canada, "About the OPC," Government of Canada. Accessed September 10, 2025, https://www.priv.gc.ca/en/

Ombudsman model that emphasises accessibility and informality.[29] Within this framework, the Commissioner may investigate complaints and review organisational practices but lacks direct order-making authority. Its jurisdiction was subsequently extended to cover the private sector with the enactment of PIPEDA.[30] This institutional design has profoundly shaped Canada's enforcement culture, privileging dialogue, guidance, and voluntary compliance over coercive sanctions.[31]

The Act outlines a structured process for handling complaints and inquiries. Proceedings may begin with a complaint from an individual, but the Commissioner also has discretion to initiate investigations on their own motion where systemic risks are suspected. Complaints deemed suitable for informal resolution may be addressed through early resolution mechanisms or mediation. More complex cases proceed to a formal inquiry, during which organisations are notified, evidence is collected, and consultations are undertaken. At the conclusion, the OPC issues a report of findings, which may include recommendations for corrective action. While these recommendations are not binding, they often carry reputational weight, and the Commissioner may apply to the Federal Court for an enforceable order, including remedies such as damages to affected individuals.

In addition to investigations, the OPC can enter into **compliance agreements**, a tool introduced in 2015, which allows organisations to formally commit to remedial measures under monitoring by the Commissioner. These agreements provide a cooperative means of securing future compliance but, like findings, they stop short of imposing penalties.

Although the OPC can conduct investigations, issue reports, and publish findings, its lack of binding sanctioning powers significantly constrains its deterrent impact. Its authority rests primarily on reputational mechanisms, including naming organisations in public reports, mobilising media attention, and seeking court oversight when cooperation fails. Recognising these structural limits, the Canadian government has proposed legislative reform through Bill C-27, which would replace PIPEDA with the *Consumer Privacy Protection Act* (CPPA).[32] The CPPA would empower the OPC with order-making capacity and administrative monetary penalties of up to the greater of CAD $10 million or 3% of global annual revenue, thereby bringing Canadian enforcement closer to global norms. Until such reforms are enacted, however, Canada's model remains comparatively restrained, relying more on persuasion than coercion in addressing entrenched corporate data practices.

By contrast, PIPEDA's reliance on the Ombudsman model, non-binding findings, and reputational pressure has cultivated an enforcement style that emphasises cooperation and education rather

---

[29] Valerie Steeves, "Privacy Law Reform in Canada," *in Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, edited by Ian Kerr et al., 360-380 (Oxford University Press, 2009).

[30] Industry Canada. *The Personal Information Protection and Electronic Documents Act: A Comprehensive Overview* (Government of Canada, 2001).

[31] Office of the Privacy Commissioner of Canada, *PIPEDA Report of Findings #2019-001,* April 9, 2019, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-001/.

[32] Canada, Bill C-27: *An Act to Enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to Make Consequential and Related Amendments to other Acts.* House of Commons, November 4, 2022, Government of Canada, https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c27_1.html

than coercion. This softer model highlights the institutional asymmetry between Canada and Nigeria, foreshadowing the divergent enforcement practices explored in the next section.

3. Enforcement in Action: Nigeria and Canada Compared

The preceding discussion outlined the institutional design and statutory powers of the NDPC and OPC, which already suggest divergent enforcement cultures: Nigeria's regime being formally equipped with coercive sanctions and Canada's regime is structured around an Ombudsman model of persuasion. The contrast becomes sharper when one examines how each authority has applied these powers in practice. The NDPC has relied on high-profile sanctions and public exposure to signal its authority and deter non-compliance, while the OPC has pursued cooperative strategies that privilege transparency, compliance agreements, and sector-wide education. The following case studies illustrate how this enforcement philosophies have been operationalised, and what they reveal about the strengths and weaknesses of each model.

3.1. NDPC Investigations and Enforcement Practice

In August 2025, the NDPC sanctioned MultiChoice Nigeria for violating the NDP Act following an investigation into privacy rights breaches and unlawful cross-border data transfers. According to the Commission's press release, the scope of MultiChoice's data processing was deemed "patently intrusive, unfair, unnecessary, and disproportionate."[33] The NDPC concluded that the company had infringed the rights of both subscribers and non-subscribers, ultimately imposing a fine of ₦766,242,500 (Seven Hundred and Sixty-Six Million, Two Hundred and Forty-Two Thousand, Five Hundred Naira). The sanction rested not only on the substantive violations but also on the company's inadequate implementation of remedial measures previously directed by the NDPC and its lack of cooperation during the regulatory process.

Beyond this individual case, the NDPC attracted wider attention through its sector-wide investigations and its unprecedented publication of over 1,000 organisations across finance, insurance, gaming, and other sectors that had failed to meet statutory audit-filing obligations.[34] These entities were given 21 days to demonstrate compliance by providing evidence of audit submissions, appointment of a Data Protection Officer (DPO), summary of technical and organisational safeguards, and registration as Data Controllers or Processors of Major Importance. Failure to comply risked enforcement orders, administrative fines, and even criminal prosecution. By publicising these defaults, the NDPC signaled a willingness to use visibility as a regulatory tool deploying reputational pressure to accelerate compliance.

This "naming and shaming" strategy reflects both ambition and risk. On one hand, it positions the NDPC as a decisive regulator unwilling to tolerate non-compliance, particularly in a jurisdiction where institutional trust is still consolidating. On the other, blanket exposure raises questions of procedural fairness, proportionality, and the risk of incentivising checkbox compliance rather than substantive accountability. Scholars of regulatory governance caution that excessive reliance on

[33] NDPC, "Press Release: Multichoice Nigeria."
[34] "NDPC Cracks down on 1, 369 Nigerian Firms."

public sanctions can amount to regulatory theater symbolic displays of authority that may undermine due process and long-term trust if not carefully calibrated.[35]

The NDPC Commissioner has sought to temper such concerns, repeatedly emphasising a remediation-first philosophy in public statements and reserving harsher sanctions for cases of willful non-compliance or systemic violations. Enforcement decisions, the Commission notes, are guided by extenuating factors such as the severity of the breach, the number of individuals affected, and the potential economic impact. In practice, this means organisations are often given corrective measures and opportunities to cure deficiencies before punitive action is imposed.[36] The MultiChoice case, however, illustrates that when remediation is ignored or cooperation withheld, the NDPC is prepared to escalate decisively to sanctions. This tiered posture oscillating between remediation and deterrence demonstrates the Commission's dual role as both educator and enforcer, though the balance between these roles remains contested.

3.2. The OPC in Action: Oversight Through Investigations

In contrast to the NDPC's sanction-oriented posture, the OPC has approached systemic non-compliance with greater caution, reflecting its reliance on persuasion and reputational leverage. Two high-profile investigations into Facebook and Equifax underscore both the OPC's capacity to expose major privacy failings and the structural limits of its enforcement regime under PIPEDA.

The Facebook inquiry, conducted jointly with the Information and Privacy Commissioner of Alberta in 2018, examined the company's facilitation of third-party applications such as "TYDL" that harvested user data far beyond what was necessary.[37] These applications captured not only the data of direct users but also that of their contacts, which was subsequently deployed for psychographic profiling and political advertising. The OPC concluded that Facebook had contravened PIPEDA by failing to obtain meaningful consent and by abdicating accountability to third-party developers without proper oversight. The Commission further found that Facebook's safeguards were inadequate, failing to meet statutory obligations of accountability and security. Yet despite these findings, Facebook rejected the OPC's jurisdiction and refused to implement the recommended reforms, forcing the matter into Federal Court. The Court ultimately confirmed Facebook's contraventions, but the drawn-out process underscored the fragility of an enforcement model that depends on corporate cooperation or judicial intervention to secure compliance.

Facebook's regulatory history in Canada illustrates this pattern. As early as 2008, the OPC had directed the company to tighten its consent practices after a complaint by the Canadian Internet Policy and Public Interest Clinic. At that time, Facebook accepted the recommendations and implemented reforms. A decade later, however, similar issues resurfaced, suggesting that voluntary compliance without binding enforcement may deliver only temporary gains. This cyclical pattern reveals the limits of "soft law" enforcement when dealing with large, resource-rich corporations capable of resisting or delaying compliance.

---

[35] Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate.* (Oxford University Press, 1991).
[36] NDPC, Annual Report 2024.
[37] Office of the Privacy Commissioner of Canada and Information and Privacy Commissioner of British Columbia, *Joint Investigation of Facebook Inc.*, April 25, 2019. https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-002/

The Equifax breach of 2017 provides a contrasting example.[38] After personal data belonging to over 143 million individuals including approximately 19,000 Canadians was compromised, the OPC investigated Equifax Canada and its U.S. parent company. The inquiry revealed significant accountability gaps, particularly in relation to cross-border data transfers and security safeguards. Unlike Facebook, Equifax entered into a compliance agreement, committing to extensive remedial measures including adoption of a new security framework, additional staffing, and independent audits overseen by the OPC. This outcome demonstrated the value of compliance agreements as cooperative tools, but also raised concerns about whether negotiated remediation is sufficiently deterrent in the face of large-scale breaches affecting millions of individuals.

Following the 2018 amendment to PIPEDA introducing mandatory breach reporting, the OPC further undertook audits to evaluate compliance across sectors. Its findings were sobering: many organisations failed to maintain adequate breach records or to notify affected individuals as required.[39] Rather than publishing a list of defaulters, the OPC responded by issuing anonymised case summaries, sector-wide guidance, and educational outreach. This approach reflects the regulator's commitment to systemic learning and trust-building, but it also illustrates its reluctance or inability to impose visible sanctions, even where compliance gaps were widespread.

Viewed in tandem, these investigations reveal a regulator committed to transparency and systemic improvement yet constrained by a legal framework that denies it coercive authority. The Facebook case demonstrates how non-binding powers can enable persistent corporate resistance, while the Equifax case highlights the potential but also the limitations of compliance agreements as cooperative remedies. The OPC's post-2018 breach audits illustrate a continued preference for education over punishment, reflecting an enforcement culture built on partnership rather than deterrence. While this approach has fostered trust among regulated entities, critics contend that it risks regulatory irrelevance in the face of repeat violations by powerful actors.

Juxtaposing the NDPC's and OPC's enforcement practices highlights the starkly different philosophies that underpin their regulatory models. Nigeria's NDPC has embraced a visibility-driven strategy, relying on sanctions, public exposure, and sector-wide investigations to signal authority and accelerate compliance in a nascent regime. By contrast, Canada's OPC has relied on the moral force of transparency, education, and negotiated remediation to promote compliance in a mature regulatory environment, but without the deterrent power of binding sanctions. Each approach carries clear strengths and vulnerabilities: the NDPC's assertiveness risks over-deterrence and due process concerns, while the OPC's restraint fosters trust but risks under-enforcement and cyclical non-compliance. These cases demonstrate the enduring tension between deterrence and cooperation in data protection enforcement, setting the stage for a deeper examination of how culture, capacity, and statutory design shape compliance outcomes.

[38] Office of the Privacy Commissioner of Canada, "Investigation into Equifax Inc. and Equifax Canada Co's Compliance with PIPEDA in Light of 2017 Breach," April 9, 2019. https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-001/

[39] OPC, *PIPEDA Report of Findings* #2019-001.

4. Critical Reflections: Culture, Capacity and Compliance

The divergent enforcement styles of the NDPC and OPC can be traced to three interrelated variables.

First, **regulatory maturity and institutional trust** shape how enforcement is deployed. Nigeria's data protection framework remains in an early stage of development, situated within a governance environment that is still consolidating institutional credibility. In this setting, public enforcement is not only a mechanism of compliance but also a tool for signaling regulatory authority and building visibility. By contrast, Canada's longer tradition of administrative law and institutional independence has cultivated a more cautious approach, where procedural fairness and reputational safeguards are prioritised, particularly given the weight of reputational consequences.

Second, **statutory infrastructure and legal authority** reveal a striking asymmetry. The NDP Act explicitly endows the NDPC with the power to impose administrative fines, issue compliance directives, and publish enforcement actions. PIPEDA, in contrast, withholds comparable sanctioning powers from the OPC, restricting its capacity to adopt an assertive enforcement posture even in cases of significant corporate misconduct. Although Bill C-27's Consumer Privacy Protection Act (CPPA) promised to close this gap by introducing order-making powers and monetary penalties, its death in late 2024 following parliamentary prorogation underscores the fragility of Canada's reform trajectory. In practical terms, this leaves Canada's federal privacy enforcement comparatively constrained, while Nigeria moves toward an expansive, penalty-driven model.

Third, **enforcement philosophy** highlights a tension between deterrence and cooperation. Nigeria's NDPC has relied heavily on visible sanctions and sector-wide exposure, treating reputational accountability as a lever to accelerate compliance uptake. Canada's OPC, by contrast, has adhered to an Ombudsman-style approach that privileges dialogue, guidance, and education. Each approach has strengths and liabilities: deterrence may secure immediate behavioral change but risks alienating stakeholders and eroding trust, while cooperation fosters long-term relationships but may appear too lenient in addressing systemic violations.

These divergences map neatly onto the broader literature on **responsive regulation,** often conceptualised as a pyramid that begins with persuasion and escalates to punitive sanctioning.[40] Nigeria has quickly moved toward the apex, using financial penalties and reputational exposure to consolidate its legitimacy. Canada, conversely, has remained closer to the base, relying on moral suasion and voluntary compliance. Both positions are defensible within the responsive regulation model, but each also illustrates the perils of imbalance: over-deterrence can undermine procedural legitimacy, while over-persuasion risks regulatory irrelevance. The policy challenge, therefore, is not to abandon either orientation but to recalibrate enforcement in ways that remain proportionate, context-sensitive, and sustainable over time.

[40] Colin Bennet and Charles Raab, *The Governance of Privacy: Policy instruments in Global Perspective*. 2nd ed. (Cambridge, MIT Press, 2006).

5. Recalibrating Enforcement: A Policy Framework for Context-Aware Compliance.

The contrasting enforcement trajectories of Nigeria and Canada highlight the urgent need for regulatory frameworks that are simultaneously effective, procedurally fair, and sensitive to institutional and sectoral realities. Enforcement cannot remain uniform across contexts; it must evolve in step with the maturity of the regulator, the diversity of regulated sectors, and the risks inherent in contemporary data economies. A more balanced paradigm requires moving beyond visibility or restraint alone, instead combining elements of deterrence and cooperation to sustain both compliance and legitimacy.

In Nigeria, the NDPC has made commendable progress in establishing its authority and embedding visibility into its compliance culture. High-profile sanctions, such as the MultiChoice Nigeria case, and the public naming of more than 1,000 non-compliant organisations have demonstrated regulatory resolve. Yet this assertiveness sits uneasily alongside the Commission's stated commitment to a remediation-first philosophy, revealing a dual role for visibility: both as a deterrent and as a signal of institutional strength. Over-reliance on reputational sanctioning, however, risks incentivising cosmetic compliance and raises questions of predictability and procedural fairness. A more sustainable framework would introduce a tiered enforcement ladder, reserving public exposure for repeat or high-risk offenders while allowing administrative lapses to be addressed through remediation windows. Codified enforcement protocols specifying timelines, reporting standards, and penalty thresholds would further reduce arbitrariness and improve certainty. Finally, reinforcing DPCO oversight through periodic quality audits, performance-linked reviews, and sanctions for superficial audits would help shift Nigeria's compliance culture from tick-box exercises to demonstrable privacy accountability.

Canada's OPC, by contrast, has cultivated trust and procedural fairness but remains structurally constrained by the absence of binding authority. Its reliance on guidance and reputational tools has built cooperative relationships with regulated entities, yet its inability to impose sanctions undermines its deterrent capacity, particularly in high-risk sectors such as finance, digital advertising, and surveillance technologies. Legislative reform is therefore imperative. Passage of the CPPA would provide the OPC with order-making powers and administrative monetary penalties, finally aligning Canadian enforcement with international standards. In addition, Canada should experiment with graduated naming protocols that publicly identify repeat or egregious offenders, thereby injecting reputational accountability into sectors resistant to voluntary compliance. Expanding proactive engagement infrastructures, compliance clinics, pre-investigation dialogues for SMEs, and regulatory sandboxes for emerging technologies would further balance deterrence with collaborative governance.

Beyond jurisdictional differences, both Nigeria and Canada must converge on systemic reforms that reinforce transparency, fairness, and adaptive governance. Embedding procedural safeguards such as standardised notice periods, response timelines, and independent appeal pathways would strengthen due process across the enforcement lifecycle. Public-facing dashboards that aggregate and anonymise enforcement trends could enhance transparency without compromising confidentiality, informing both regulated entities and the broader public. Finally, investing in co-regulatory ecosystems through sectoral codes of practice, civil society partnerships, and targeted capacity-building initiatives would help embed compliance as a shared societal norm rather than a mere legal obligation.

Recalibrating enforcement in this manner does not entail collapsing the distinction between deterrence and cooperation. Rather, it acknowledges that both are indispensable and that their effectiveness depends on proportionality, timing, and institutional context. A rights-respecting, context-sensitive, and adaptive enforcement paradigm offers the best path toward sustaining regulatory legitimacy and accountability in the rapidly evolving terrain of global data protection.

6. Conclusion

This paper has examined the enforcement architectures of the NDPC and OPC as reflections of divergent regulatory cultures, statutory powers, and strategic philosophies. Nigeria's NDPC, while formally committed to remediation, has relied heavily on sanctions and public exposure, using visibility as both deterrent and institutional signal. Canada's OPC, by contrast, has embraced a cooperative model centered on guidance, transparency, and moral persuasion. Each trajectory has yielded benefits, yet each reveals vulnerabilities: over-deterrence in Nigeria risks undermining procedural fairness, while under-enforcement in Canada threatens regulatory credibility.

The future of effective data protection does not lie in privileging one model over the other, but in synthesising their strengths. Sanctions must be proportionate and tempered by procedural safeguards; cooperative engagement must be underpinned by credible deterrence; and public visibility must serve legitimacy rather than spectacle. In an era defined by algorithmic harms, cross-border data flows, and intensifying privacy risks, regulators require not a single instrument but an integrated toolkit: legal, institutional, and reputational to sustain authority and accountability.

By juxtaposing Nigeria's emergent, visibility-driven enforcement with Canada's restrained, partnership-oriented approach, this paper advances comparative privacy scholarship and offers a policy-relevant insight: sustainable compliance cultures are forged not through deterrence or cooperation alone, but through adaptive enforcement architectures that balance both in contextually grounded and procedurally fair way.

Regulatory Compliance: Best Practices, Challenges and Enforcement under the Nigeria Data Protection Act (NDP Act), and Global Frameworks (GDPR, etc.)

Olayinka Arasi, Esq.[41] Messiah Iheanacho, Esq.[42] Jamilah Aliyu, Esq.[43]

ABSTRACT

Nigeria's digital economy is growing, hence the youthful population and her ever-growing technology sector have equally created an urgency and need to safeguard personal data. The Nigeria Data Protection Regulation, 2019 (NDPR) and the enacted Nigeria Data Protection Act 2023, marked some strategic gains in institutionalising data protection and aligning Nigeria with global frameworks like the European Union's General Data Protection Regulation (GDPR). Still, compliance and enforcement remain a problem. This research interrogates the intersection between best practices, systemic gaps and enforcement realities under the NDP Act, while comparing Nigeria's data protection framework with other, broader, international standards. It implores comparative analysis, literature review and case law, to highlight certain barriers to effective compliance, including factors like limited public awareness, under-resourced regulators, inadequate institutional coordination and cultural attitudes toward privacy. The research also examines the NDP Act's potential as a driving force for innovation and trust in digital services, particularly in sectors like fintech, health-consulting and e-commerce, where secure data flows are very critical to operation. The research paper concludes with some practical recommendations, including capacity building for the Nigeria Data Protection Commission (NDPC), enhanced cross-border cooperation, sector-specific compliance guidance and sustained public education, showing how bridging regulatory intent with effective practice can strengthen Nigeria's data protection regime and position her as a continental leader in digital governance.

Keywords: Nigeria Data Protection Act (NDP Act); GDPR; Compliance and Enforcement; Digital Economy; Data Governance

[41] olayinka.arasi@solinagroup.com
Solina Centre for International Development and Research (SCIDaR)
[42] messiah.iheanacho@solinagroup.com
Solina Centre for International Development and Research (SCIDaR)
[43] jamilah.aliyu@solinagroup.com
Solina Centre for International Development and Research (SCIDaR)

1. Introduction

The value of the digital economy cannot be understated. The use of digital technology has shaped economic activities, from the production and marketing of goods and services, to consumption of these outputs through online platforms and networks. In Africa, this transformation is especially visible in Nigeria, where the youthful, entrepreneurial and technology-driven population is harnessing digital tools to reshape finance, commerce, education and healthcare. Nigeria's digital economy revenues grew from $5.09 billion in 2019 to nearly $10 billion in 2021[44], and there are projections of exceeding $18 billion by 2026. This momentum is reinforced by Nigeria's position as the leading destination for technology start-up investment in Africa, outpacing South Africa, Kenya, Egypt and neighboring Ghana. Yet, beneath these figures, there's a fragile ecosystem marked by gaps in infrastructure, policy coherence and regulatory enforcement, hindering Nigeria's ambition to lead Africa's digital transformation.

Every sustainable digital economy needs trust. Both the regulators and subjects need to be certain that data generated and shared across platforms is protected, used responsibly and governed within a clearly outlined legal framework. Hence, Nigeria took a decisive step in 2019 by issuing the Nigeria Data Protection Regulation (NDPR)[45]. This was the first significant attempt at codifying personal data protection. The NDPR created compliance obligations for data controllers and processors, mandated audits and introduced sanctions for data breaches. However, regulation became difficult, as it relied heavily on subsidiary regulations and oversight powers of the National Information Technology Development Agency (NITDA), which lacked independence and resources to enforce effective compliance.

Eventually, the enactment of the Nigeria Data Protection Act[46], 2023 marked a change in the data protection ecosystem[47]. Unlike the NDPR, the NDP Act provided statutory authority for data governance and established the Nigeria Data Protection Commission (NDPC) as an independent regulator, with codified rights for data subjects. It also aligns closely with international best practices, particularly the European Union's General Data Protection Regulation (GDPR)[48], which is regarded globally as the gold standard for data protection.

The compliance environment did not stop with the NDP Act. The General Application and Implementation Directive (GAID), 2025[49] was introduced as a complementary instrument to operationalise most of the NDP Act's provisions. GAID provides clarity on compliance obligations, enforcement procedures and sector-specific applications, to see the actualisation of the intention of the act. Much like interpretative directives under the GDPR, GAID acts as a bridge between

---

[44] Olugbenga Agboola, "Nigeria's Budding Digital Economy: Coping with Disruptive Technology" *Central Bank of Nigeria*, December 4, 2022, https://dc.cbn.gov.ng/efr/vol60/iss4/6/

[45] National Information Technology Development Agency (NITDA), Nigeria Data Protection Regulation (NDPR) (Abuja: NITDA, 2019)

[46] Federal Republic of Nigeria, Nigeria Data Protection Act, 2023 (Abuja: Government of the Federal Republic of Nigeria).

[47] Olumide Babalola, "Nigeria's Data Protection Legal and Institutional Model: An Overview," International Data Privacy Law 12, no. 1 (2022): 44–60

[48] European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), Official Journal of the European Union, L 119, 4 May 2016, 1–88.

[49] Nigeria, General Application and Implementation Directive (GAID), 2025, issued by the Nigeria Data Protection Commission (NDPC)

law and practice, assisting organisations in understanding their responsibilities while strengthening the ability to drive enforcement.

This research places the NDP Act within the wider scope of global data protection, and drops comparative lessons from the GDPR and other frameworks. It also explores the compliance obligations imposed on organisations, the gaps in enforcement and challenges regulators face in ensuring accountability.

1.1 Research Objectives

i. To examine compliance obligations under the NDP Act.
ii. To compare the NDP Act with GDPR and other global frameworks.
iii. To identify challenges in enforcement and compliance.
iv. To recommend best practices for regulators, organisations and data controllers.

2. Theoretical Framework

This research analyses regulatory compliance under the NDP Act[50], the way it functions with the GAID[51], and its comparative positioning against global frameworks like the GDPR[52]. The framework for this research is divided into:

a. Theories of Regulation: Command-and-Control vs. Risk-Based Approaches

Traditionally, the command-and-control model is the most known regulatory practice. In the context of data protection, there are mandatory audits, detailed consent requirements and fixed penalties for breaches. The NDPR largely reflected this approach, by providing obligations without much flexibility for innovation or even sectoral nuance.

By contrast, risk-based regulation emphasises proportionality. It allows organisations to assess and mitigate risks according to the sensitivity of the data they handle. Both regimes adopt this approach, but with slight variations: the GDPR mandates Data Protection Impact Assessments (DPIAs) for high-risk processing, while the NDP Act requires Data Privacy Impact Assessments for similarly risky activities. In both cases, the aim is to embed privacy by design and ensure that risks are addressed before processing begins.

b. The Principle of Accountability in Data Protection Law

Modern data protection framework upholds the principle of accountability. Under GDPR Article 5(2),[53] data controllers are not only responsible for compliance but must show that they understand what it entails.

For Nigeria, accountability is crucial because regulatory resources are limited. The NDP Act requires data controllers to implement technical and organisational measures, conduct periodic audits and appoint a data protection officer in certain cases[54]. GAID reinforces these duties by prescribing practical steps for demonstrating compliance, like record-keeping, training and timely breach notification[55].

---

[50] NDP Act, 2023
[51] GAID, 2025
[52] GDPR, 2016
[53] General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, Art. 5(2)
[54] Nigeria Data Protection Act (NDP Act), 2023, SS. 31–33
[55] GAID, 2025, Pt. III

c. Data Subject Rights as Human Rights

This theoretical foundation arises from the recognition of data subject rights as extensions of human rights. Privacy is enshrined in international human rights law, like **Article 12 of the Universal Declaration of Human Rights**[56] and **Article 17 of the International Covenant on Civil and Political Rights.**[57] In Nigeria, **Section 37 of the 1999 Constitution** protects the right to privacy, governing how correspondence, telephone conversations and communications are handled[58].

The GDPR and NDP Act extend these rights into the digital age by codifying specific entitlements like right of access, rectification, erasure, data portability and objection to processing. These rights give individuals powers to control how their personal data is collected, stored and used, reflecting the broader human rights principle of autonomy. By situating data protection within human rights discourse, the NDP Act reiterates that privacy is a compliance issue as well as a fundamental right that regulators, organisations and courts must strive to protect[59].

d. Comparative Compliance Theory: Global vs. Localized Application

Lastly, this theory provides Nigeria the opportunity to evaluate her data protection framework against global standards. There is a problem in trying to balance global convergence and local adaptation. On one hand, harmonizing the local framework with global standards like GDPR enables interoperability and facilitates cross-border trade, it also enhances Nigeria's chances of securing decisions to assist international data flows. But on the other hand, regulatory transplantation without adaptation might result in ignoring local realities, like resource constraints and lack of enforcement capacity. Comparative compliance theory helps us to appreciate the need for contextual localization.

3. Overview of Legal and Regulatory Frameworks

As economies and societies become increasingly data-driven, legal frameworks are also evolving to protect individual rights and ensure organisational accountability to enable cross-border data flows under conditions of trust. This section provides an overview of the Nigerian sector operating under the NDP Act[60] and the GAID[61], placing them within the broader global landscape like the **EU's General Data Protection Regulation (GDPR)**[62], the **California Consumer Privacy Act (CCPA)**[63], South Africa's **Protection of Personal Information Act (POPIA)**[64]**,** and **UK Data (Use and Access) Act 2025**[65].

---

[56] Universal Declaration of Human Rights, adopted December 10, 1948, United Nations General Assembly Resolution 217 A (III), Art. 12
[57] International Covenant on Civil and Political Rights (ICCPR), adopted December 16, 1966, entered into force March 23, 1976, 999 U.N.T.S. 171, Art. 17
[58] Constitution of the Federal Republic of Nigeria, CFRN 1999 (as amended), S. 37
[59] Nigeria Data Protection Act (NDP Act), 2023, SS. 2–3
[60] NDP Act, 2023
[61] GAID, 2025
[62] GDPR, 2016
[63] California Consumer Privacy Act of 2018, Cal. Civ. Code S 1798.100–1798.199
[64] Protection of Personal Information Act 4 of 2013 (South Africa)
[65] Data (Use and Access) Act 2025, c. 18 (UK)

3.1 Nigeria Data Protection Act (NDP Act)[66]

The NDP Act is Nigeria's first comprehensive statutory intervention in data protection. It replaced the Nigeria Data Protection Regulation (NDPR) of 2019[67], which, though significant, was limited by its regulatory pedigree as a subsidiary instrument and its reliance on the National Information Technology Development Agency (NITDA)[68] as its arm of enforcement. Now, the NDP Act situates data protection within the primary legislation of Nigeria, which provides it with stronger constitutional and institutional grounding. At its core, the NDP Act articulates certain key principles of data protection such as:

i. Lawful, fair and transparent processing of personal data.
ii. Purpose limitation.
iii. Data minimisation.
iv. Data Accuracy.
v. Storage limitation.
vi. Integrity and confidentiality.

Under the NDP Act, the NDPC acts as an independent regulatory authority. As a watchdog, the Commission is tasked with monitoring compliance, investigating complaints, issuing compliance orders and imposing penalties.

3.2 General Application and Implementation Directive (GAID, 2025)[69]

While the NDP Act lays down the statutory framework, it is trite that effective regulation requires operational clarity. Thus, the General Application and Implementation Directive (GAID, 2025), a regulatory instrument issued by the Nigeria Data Protection Commission (NDPC) on March 20, 2025, provides detailed guidance for implementing the Nigeria Data Protection Act (NDP Act) 2023[70]. It became effective September 19, 2025, and functions as a subordinate yet binding instrument under the NDP Act.

The legal nature of GAID is similar to regulatory directives in other jurisdictions, such as guidelines issued under the GDPR by the European Data Protection Board (EDPB)[71]. It is important to note that it does not create new rights or duties beyond the NDP Act, but clarifies how existing provisions should be applied in practice. For example, GAID specifies reporting timelines for data breaches, minimum requirements for Data Protection Officers (DPOs), and sector-specific compliance templates for industries such as finance, health and telecommunications[72].

3.3 Global Frameworks for Benchmarking

To fully appreciate Nigeria's evolving data protection structure, it is necessary to situate it within the global landscape. Three frameworks are particularly relevant:

---

[66] NDP Act, 2023
[67] NDPR, 2019
[68] National Information Technology Development Agency (NITDA), Nigeria
[69] GAID, 2025
[70] NDP Act, 2023
[71] European Data Protection Board (EDPB)
[72] General Application and Implementation Directive (GAID), 2025, Nigeria Data Protection Commission (NDPC), Art 11-12, Art 33, Schedule 2

a. The GDPR (2016/2018) is widely regarded as the global gold standard in data protection[73]. Its widespread reach, detailed rights of data subjects and rigorous enforcement mechanisms have set the benchmark for national legislation worldwide. The GDPR's innovations include the principle of privacy by design and by default, the risk-based approach to regulation and a strong accountability framework. The NDP Act[74] mirrors many of these features, including creating an independent regulator, codifying data subject rights and creating rules for when data has to be transferred across border.

b. The **California Consumer Privacy Act (CCPA, 2018)**[75] represents a distinct approach rooted in U.S. consumer rights law. Unlike the GDPR's consent-based model, the CCPA primarily operates on an opt-out basis, granting consumers the right to request disclosure, deletion and non-sale of their personal information[76]. While narrower in scope, the CCPA reflects the growing global consensus that individuals must have agency over their personal data. The CCPA offers Nigeria lessons in consumer-driven enforcement, though its market-driven orientation differs significantly from the rights-based framework of the NDP Act[77].

c. South Africa's **Protection of Personal Information Act (POPIA, 2013; effective 2021)**[78] provides a regional comparator for this research. POPIA establishes an independent regulator and codifies principles similar to those in the GDPR. It reflects an African approach to embedding privacy within constitutional values. Its gradual implementation also underscores the challenges African states face in transitioning from legislation to actual practice. Compared to POPIA, the NDP Act benefits from a more recent alignment with GDPR principles, but faces similar constraints like institutional capacity, public awareness and enforcement.

To further illustrate the points of convergence and divergence between Nigeria's emerging data protection framework and other global standards, the table below provides a comparative overview.

Feature	NDP Act, 2023	GAID, 2025	GDPR, 2018	CCPA, 2020	POPIA, 2021
Legal Nature	Primary legislation establishing comprehensive data protection	Directive issued under NDP Act for standardised compliance and enforcement	Regulation directly binding across EU Member States	State law specific to California, U.S.	National legislation harmonising with global norms
Supervisory Authority	Nigeria Data Protection Commission (NDPC)	NDPC (with GAID as operational guidance)	Data Protection Authorities (DPAs) in each EU country,	California Privacy Protection Agency (CPPA) and	Information Regulator of South Africa

[73] European Union, General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, adopted April 27, 2016, effective May 25, 2018
[74] NDP Act, 2023
[75] California Consumer Privacy Act of 2018, Cal. Civ. Code S. 1798.100–1798.199 (2018)
[76] CCPA, Cal. Civ. Code S. 1798.100–1798.120
[77] Nigeria Data Protection Act (NDP Act), 2023 Part VI S. 34-38
[78] Republic of South Africa. Protection of Personal Information Act 4 of 2013. Pretoria: Government Printer, 2013

			coordinated by EDPB[79]	Attorney General	
Core Principles	Lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, security, accountability	Reinforces NDP Act principles with detailed compliance obligations	Same as NDP Act, source of influence	Focuses on consumer rights, less emphasis on accountability principle	Largely mirrors GDPR, tailored to South African context
Data Subject Rights	Access, rectification, erasure, restriction, portability, objection, withdrawal of consent	Operationalises these rights with procedural timelines and remedies	Same as NDP Act; GDPR origin	Right to know, delete, opt-out of data sale, non-discrimination	Similar to GDPR; emphasises consent and access
Enforcement Powers	Investigations, administrative fines, corrective orders, suspension[80]	Provides enforcement guidance, thresholds for fines, structured compliance audits	Strong enforcement: heavy fines (up to €20m or 4% global turnover)[81]	Civil penalties, statutory damages, private right of action for breaches[82]	Enforcement through fines, court orders, criminal liability[83]
Penalty Structure	Tiered fines based on severity and turnover	Clarifies thresholds and processes for penalty imposition	One of the most severe globally	Moderate fines, damages through litigation	Fines capped but combined with strong compliance obligations

4. Regulatory Compliance Obligations under NDP Act

The Nigeria Data Protection Act (NDP Act) 2023[84] sets out comprehensive compliance obligations for organisations that collect, process, or store personal data within Nigeria or involving Nigerian citizens[85]. These obligations try to balance innovation in the digital economy with the constitutional right to privacy, while also aligning with international standards such as the GDPR[86]. They reflect four broad clusters:

[79] GDPR, Art. 68 (establishing the European Data Protection Board)
[80] NDP Act, Part IX (sanctions, enforcement and penalties by the NDPC)
[81] GDPR, Art. 83 (administrative fines and penalty thresholds)
[82] Cal. Civ. Code S. 1798.155 (civil penalties and enforcement under the CCPA)
[83] South Africa, POPIA, Chapter 11 (enforcement and penalties)
[84] NDP Act, 2023
[85] Nigeria, Nigeria Data Protection Act, No. 4 of 2023 (Lagos: Federal Government Printer, 2023), Part II, Sections 24–25 (general principles of processing)
[86] European Union, General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, OJ L 119/1 (2016), Art. 5, 12–23, and 32–34 (principles, rights, security and breach notification)

a. Lawful Processing Principles

The NDP Act codifies foundational principles of data protection that guide all processing activities[87]. These include lawfulness, fairness and transparency, requiring organisations to always ensure personal data is processed on a valid legal basis and in a manner the data subjects understand. Other principles like purpose limitation, data minimisation and storage limitation are put in place to prevent excessive or indefinite retention of personal data beyond legitimate business needs.

b. Data Subject Rights

The NDP Act recognises data subjects as rights-holders[88]. The Act guarantees rights of access, rectification, erasure, restriction of processing, data portability and objection to processing, along with certain rights related to automated decision-making and profiling. These rights empower individuals to exercise control over their personal data, compelling organisations to design transparent and accessible mechanisms for responding to requests.

c. Obligations of Controllers and Processors

The NDP Act differentiates between data controllers (those who determine the purposes and means of processing) and data processors (those who process data on behalf of controllers)[89]. Data controllers bear the primary responsibility of ensuring data compliance, including adopting appropriate policies, conducting **Data Protection Impact Assessments (DPIAs)** where they envisage high-risk processing, and maintaining detailed records of processing activities too. Data Processors, on the other hand, must only act on the documented instructions of controllers and put in place some equivalent safeguards[90].

d. Data Security and Breach Notification

Security is a core pillar of the NDP Act. Organisations must adopt appropriate technical and organisational measures to protect personal data from unauthorised access, loss, alteration, or unneeded disclosure[91]. The Act makes provisions form encryption, pseudonymisation, access controls, and staff training as necessary safeguards. Where a personal data breach occurs, the NDP Act also requires timely notification to both the NDPC and affected data subjects if the breach poses a significant risk to their rights and freedoms[92].

5. Best Practices for Compliance

a. Governance Structures

Governance forms the foundation of effective compliance. Acts like appointing a Data Protection Officer (DPO) or establishing a Data Governance Committee operating with a Data Governance Framework provides oversight and ensures accountability too[93]. It also creates a central point of contact with the Nigeria Data Protection Commission (NDPC)[94].

---

[87] *Ibid.*, Section 24-27 (lawfulness, fairness, transparency, purpose limitation, minimisation, storage limitation)
[88] *Ibid.*, Part III, Sections 34 (rights of data subjects, including access, rectification, erasure, restriction, portability, objection and automated decision-making)
[89] *Ibid.*, Part IV, Sections 28,29, 37 (obligations of controllers and processors, DPIAs and record-keeping)
[90] *Ibid.*, Section 39 (processors' duties to act only on controllers' instructions and ensure safeguards)
[91] *Ibid.*, Part V, Sections 40–43 (data security obligations, technical and organisational measures)
[92] *Ibid.*, Section 40 (data breach notification to NDPC and affected subjects)
[93] NDP Act 2023, S. 32 (requirement to appoint a Data Protection Officer in certain cases)
[94] NDP Act 2023, S. 5 (establishment and functions of the Nigeria Data Protection Commission)

Governance mostly entails formalising internal policies, setting escalation protocols and embedding privacy considerations into board-level decision-making of the organisation.

b. Data Inventory and Mapping

An accurate data inventory and mapping process is also critical. Organisations will not be able to protect what they do not know they hold[95]. But by identifying the types of data collected, processing purposes, storage locations and data flows, they can gain visibility over risks and apply appropriate safeguards.

c. Privacy by Design & Default

Embedding Privacy by Design and Default ensures that privacy considerations are not retrofitted but integrated from the outset of system development[96]. What this simply means is that by limiting data collection to what is necessary, minimising retention and setting privacy-friendly defaults, an application would require explicit consent before accessing location data instead of activating it by default.

d. Audit and Data Protection Impact Assessments (DPIAs)

Data Protection Impact Assessments (DPIAs) and regular audits are preventive tools that will also help organisations to evaluate risks before launching new initiatives and monitor compliance[97]. DPIAs help organisations to assess potential harm to data subjects, while audit exercises provide evidence of compliance for regulators and will help to identify areas needing improvement[98].

e. Training & Awareness

Finally, training and awareness are indispensable. As captured in the GAID, staff at all levels must understand their roles in data protection[99]. Regular training sessions, organisation-wide privacy awareness campaigns and scenario-based drills can turn compliance from a legal obligation into an offhanded organisational culture.

6. Challenges in Implementation & Enforcement

The NDP Act provides a forward-looking framework, but in practice, there are still challenges. These challenges exist both at the institutional level, where enforcement structures are still consolidating, and at the practical level, where compliance is uneven across various sectors. Some of the challenges are:

6.1 Institutional Challenges

As a relatively new regulator, the NDPC faces resource shortages, limited technical expertise and competing demands across a growing digital ecosystem. Without sufficient funding and staffing, the NDPC struggles to monitor compliance beyond high-profile corporations, this has created a loophole where several SMEs and public agencies are under-scrutinised[100].

---

[95] European Union, General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, Art. 30 (ROPA)
[96] GDPR, Art. 25 (data protection by design and by default)
[97] NDP Act 2023, S. 28 (requirement for Data Protection Impact Assessments)
[98] Nigeria Data Protection Commission, General Application and Implementation Directive (GAID), 2025, pt. IV (audit and compliance monitoring requirements)
[99] GAID 2025, Pt. V (obligations on training and capacity building)
[100] Nigeria, Nigeria Data Protection Act (NDP Act), 2023, S. 5 (establishment and powers of the NDPC)

The presence of overlapping regulators also compounds this problem. Agencies such as NITDA, the CBN and sector-specific Commissions often issue guidelines with implications for data processing. While they may have good intentions, this regulatory pluralism gives rise to confusion, duplication and regulatory arbitrage by organisations that exploit these grey zones[101].

Another challenge is the lack of judicial precedent and weak enforcement culture. Nigerian courts are still developing jurisprudence around data privacy, resulting in uncertainty over how rights and obligations will be interpreted. In the case of **Digital Rights Lawyers Initiative v. Unity Bank Plc**[102], for instance, the claimant alleged unlawful disclosure of personal data, but the court dismissed the action on the basis that the claimant failed to demonstrate a breach or specific harm. The narrow reasoning in that case illustrates why some organisations believe enforcement actions may be too technical for victims, and may not withstand legal challenge, thereby weakening deterrence[103]. Also, in the second case of **Olumide Babalola LP v. True Software Scandinavia AB & Ors**[104], the claimant alleged unlawful processing and dissemination of personal data on the Truecaller platform, a phone app used for caller identification. The Federal High Court in Abuja dismissed the suit after holding that the applicant failed to establish that Truecaller, as a platform operator, qualified as a data controller responsible for the alleged misuse of information. Rather than engage with the broader question of how digital platforms collect and disseminate personal information in Nigeria, the court adopted a narrow construction of liability and declined to infer any breach from the platform's operational model. The cumulative effect of these decisions is the emergence of a judicial culture in which data-protection claims face significant hurdles, and for many organisations, this reinforces the perception that data-protection enforcement in Nigeria is either too technical for victims to sustain in court or too underdeveloped to create any meaningful deterrence.

6.2 Practical Challenges

On the ground, compliance is hampered by low awareness among SMEs and public institutions. Many of such enterprises lack understanding of the NDP Act's requirements or resources to operationalise compliance. This creates a two-tier system where multinational firms adopt global standards while local businesses remain largely unregulated. The high cost of compliance also discourages uptake. Hiring Data Protection Officers, investing in a secure IT system and conducting regular audits is expensive for small enterprises. Most of these issues force reliance on expensive consultants[105].

6.3 Cultural Attitude Towards Privacy

In addition to institutional and resource-based barriers, cultural attitudes also undermine compliance. Privacy in Nigeria is often treated as negotiable within communal contexts, where citizens share personal details or comply with intrusive data requests from banks, telcos, or

---

[101] National Information Technology Development Agency (NITDA), Nigeria Data Protection Regulation (NDPR), 2019; Central Bank of Nigeria (CBN), Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers, 2018

[102] Digital Rights Lawyers Initiative v. Unity Bank Plc, Suit No. FHC/L/CS/1472/2020

[103] See Digital Rights Lawyers Initiative v. NIMC (FHC/ABJ/CS/1519/2020)

[104] See Olumide Babalola LP v. True Software Scandinavia AB & Ors (FHC/ABJ/CS/195/2024)

[105] European Union Agency for Cybersecurity (ENISA), Guidelines for SMEs on the security of personal data processing, (Brussels: ENISA, 2020)

government agencies. This apathy and weak consumer-rights culture discourage complaints or litigation.

The NDP Act's success will be dependent on overcoming these challenges. Until then, Nigeria's data protection sector risks lagging behind.

7. Enforcement Mechanisms

A data protection framework has to be effective in both the elegance of its drafting and the robustness of its enforcement mechanisms. As Uwadinma notes, institutional limitations, inadequate cybersecurity infrastructure and low levels of public awareness remain persistent barriers to effective implementation of the NDP Act[106]. The NDP Act recognizes this by granting the NDPC significant powers, further reinforced by the **General Application and Implementation Directive (GAID, 2025)**[107]. Together, these instruments aim to build an enforcement regime that is credible, transparent and globally interoperable.

7.1 NDPC's Powers under the NDP Act

The NDPC has authority to issue fines, penalties and corrective directives against organisations that breach directives of the NDP Act[108]. These sanctions could be warnings and compliance orders or significant administrative fines which are proportionate to the gravity of the offence. The Commission may also suspend processing activities, require data deletion, or impose remedial measures on entities found wanting[109].

7.2 GAID's Role in Clarifying Enforcement

Recent comparative studies also highlight that while Kenya has made measurable progress in privacy enforcement, Nigeria still grapples with foundational institutional and awareness challenges, underscoring the need for an African approach to regulatory practice[110]. The GAID strengthens this framework by standardising enforcement practices and clarifying interpretive ambiguities[111]. For instance, it provides operational detail on calculating fines, assessing high-risk processing and determining the thresholds for breach notifications. With this, GAID reduces regulatory uncertainty and promotes consistent enforcement across every sector, limiting chances of organisations exploiting loopholes.

7.3 Lessons from the GDPR Model

When we compare Nigeria's regime with the EU's GDPR enforcement model, we see the same reliance on high-profile sanctions to shape corporate behaviour. Under the GDPR, multi-million-

---

[106] A. I. Uwadinma, "Data Privacy and Consumer Protection in Nigeria's Digital Economy: A Legal Examination of the Nigeria Data Protection Act, 2023," Admiralty University of Nigeria Faculty of Law Working Paper (2023)
[107] Nigeria Data Protection Act (NDP Act), 2023, s. 5(1) – (3)
[108] NDP Act, 2023, S. 48 (administrative sanctions and corrective powers)
[109] NDP Act, 2023, Sections 34–38 (suspension of processing, data deletion orders)
[110] Isaac Juma and Bukola Faturoti, "Enforcing Data Privacy in Kenya and Nigeria: Towards an African Approach to Regulatory Practice," International Review of Law, Computers & Technology, May 23, 2025
[111] Nigeria Data Protection Commission (NDPC), General Application and Implementation Directive (GAID), 2025, Part IV

euro fines against companies like Meta and Amazon[112] demonstrate how meaningful penalties deter misconduct. Nigeria has begun to adopt a similar approach by imposing significant fines on large organisations[113], and has, in the past, publicised some of these sanctions to reinforce compliance expectations. Sustaining this model of transparent enforcement will further strengthen the credibility of the NDP Act.

7.4 Comparative Note on the UK Data (Use and Access) Act 2025

The recent enactment of the UK Data (Use and Access) Act 2025 (DUAA)[114] also provides some useful comparative insights for Nigeria. It refines aspects of the UK GDPR and introduces some targeted measures aimed at improving data accessibility, security and innovation. It has provisions for flexible adequacy test for international transfers, a list of recognized legitimate interests, by requiring only reasonable and proportionate searches. It also provides rules on automated decision-making, provided transparency and human review mechanisms[115].

Most importantly are the DUAA's provisions on smart data schemes, which extend the concept of data portability beyond personal data into non-personal and sector-specific contexts such as banking, energy and telecommunications. This legislation which was inspired by the success of open banking and seeks to drive competition and innovation while embedding clear compliance and complaint-handling obligations for practicing firms.[116]

The NDP Act could draw lessons from here, especially as artificial intelligence and automated processing becomes central to service delivery, and also embed safeguards on automated decision-making to help strengthen trust in Nigeria's digital economy[117].

7.5 Data Subject Complaints & Redress

Under the NDP Act, data subjects can lodge complaints directly with the NDPC, and it must investigate and sanction erring organisations[118]. Judicial channels have also helped to provide redress. In **Digital Rights Lawyers Initiative v. National Identity Management Commission & Anor**[119], the court entertained claims regarding data protection breaches under the NDPR, stating that individuals may seek judicial enforcement of privacy rights in addition to regulatory complaints.

7.6 International Cooperation

Finally, enforcement cannot be restricted to national borders. With cross-border data flows integral to modern commerce, the NDPC must engage in international cooperation with

---

[112] European Data Protection Board (EDPB), "Decision on Meta Platforms Ireland Ltd.," 2023; Commission Nationale de l'Informatique et des Libertés (CNIL), CNIL fines Amazon Europe Core €35 million, 2020

[113] https://www.dataguidance.com/news/nigeria-ndpc-fines-multichoice-nigeria-ngn-766m

[114] United Kingdom, Data (Use and Access) Act 2025 (U.K.). The Act came into force in June 2025 and will be phased in through 2026

[115] Francesca Blythe, Eleanor Dodding, and Paida Manhambara, "The UK Data (Use and Access) Act 2025: Implications for Financial Services," Sidley Austin LLP, July 30, 2025

[116] UK Government, "Guidance: Data (Use and Access) Act 2025," GOV.UK, 2025

[117] UK Information Commissioner's Office (ICO), "Overview of the Data (Use and Access) Act 2025," 2025

[118] NDP Act, 2023, s. 46–53(complaints and redress procedures)

[119] Digital Rights Lawyers Initiative v. National Identity Management Commission, Suit No. FHC/ABJ/CS/136/2020

regulators in Europe, the U.S., and other jurisdictions[120]. The NDPC has already taken steps in this direction as it has signed cooperation MoUs with bodies such as the Office of the Privacy Commissioner of Canada and the Dubai International Financial Centre Authority, and participates actively in global networks, including the Global Privacy Assembly (GPA) and the Global Cross-Border Privacy Rules (CBPR) Forum. This collaboration is useful as it encourages mutual recognition of adequacy, coordinated investigations and enforcement of sanctions against multinationals operating across jurisdictions.

8. Recommendations

The NDP Act has laid the groundwork for credible digital rights, but its success will depend on how quickly the gaps in capacity, awareness and enforcement are addressed. Below are some useful recommendations:

a. There should be adequate funding, operational independence and recruitment of skilled experts in law, cybersecurity and digital forensics for effective oversight.
b. Compliance challenges vary across industries, hence the NDPC should issue sector-specific guidelines. Financial services grapple with anti-money laundering overlaps, health institutions manage sensitive medical data, while ed-tech and fintech startups face resource constraints.
c. Incentivising SMEs is critical to broaden compliance uptake. Rather than relying solely on penalties, regulators could introduce simplified compliance toolkits, phased implementation timelines, or tax incentives for firms that demonstrate good data governance.
d. Public awareness and digital literacy also require deliberate investment. Citizens must understand their rights to demand accountability from controllers and processors. Regular campaigns, partnerships with civil society and integration of data protection into organisational by-laws could build a culture where privacy is valued as a public good.
e. Lastly, Nigeria needs to develop case law and judicial activism around data protection. Clear judicial interpretation will anchor enforcement and build precedents that deter misconduct. There should be training programmes for judges, creation of specialised data protection courts or tribunals, and publication of landmark rulings to strengthen the judiciary's role.

9. Conclusion

In today's digital economy, data privacy is a global imperative. From social interactions to financial transactions, personal data is now the currency of trust. Misusing this trust carries profound social and economic costs. In line with this, the NDP Act is rightly celebrated as a landmark achievement. It places Nigeria within the community of nations that recognise data rights as integral to human dignity and sustainable development. And just as laws that remain static quickly lose relevance in the face of fast-moving technologies, for instance, artificial intelligence, big data and cross-border digital trade, embedding some of these best practices, from governance structures to privacy by design, are essential to ensure resilience through the test of time.

---

[120] African Union, African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), 2014, Art. 25

Regulating Children's Interactions with AI: Privacy, Safety, and Social Impact

Gilbert Obichere
Interim Head of AI Governance, African Institute for Artificial Intelligence
Gilbert.Obichere@AI-4AI.org

ABSTRACT

Artificial intelligence (AI) is playing an increasingly prominent role in the lives of children and adolescents, influencing their experiences in education, entertainment, social media, and healthcare. With chatbots becoming more socially responsive, young users are beginning to form intimate and therapeutic relationships with these AI systems. A 2024 study published by the National Library of Medicine found that approximately 28% of respondents have used AI for quick support or as a personal therapist.[121] Similarly, a recent report by Common Sense Media revealed that 72% of teenagers aged 13 to 17 have engaged with AI companions at least once, with 18% using AI for conversation and social practice, 12% for emotional and mental health support, and 9% considering AI as a friend or best friend.[122] The use of AI as a therapeutic agent by minors raises significant concerns. In one tragic case, the parents of a teenager who died by suicide sued OpenAI, alleging that ChatGPT suggested methods for self-harm.[123] Governments and international organisations have been making concerted efforts towards protecting young people from AI-related harms. However, current governance frameworks remain fragmented, uneven across jurisdictions, and largely reactive. This paper situates the regulation of children's interactions with AI at the intersection of privacy, safety, and societal implications. It maps existing frameworks, highlights governance gaps, and proposes pathways toward child-centred AI governance.

Keywords: AI, Children, Safety, Frameworks, Regulation

[121] Alyssa Hunt, "Can I Use AI as My Therapist? The Truth about Turning to Chatbots for Therapy" (Loma Linda University Health, 2025), https://news.llu.edu/health-wellness/can-i-use-ai-my-therapist-truth-about-turning-chatbots-therapy (accessed September 7, 2025).
[122] Gili Malinsky, "AI Can't Be Your Therapist: 'These Bots Basically Tell People Exactly What They Want to Hear,' Psychologist Says" (CNBC, July 17, 2025), https://www.cnbc.com/2025/07/17/ai-cant-replace-human-relationships-especially-not-a-therapist (accessed September 7, 2025).
[123] CNN, *"Parents of 16-Year-Old Sue OpenAI Alleging ChatGPT Assisted Son's Suicide"* (CNN, August 26, 2025), https://edition.cnn.com/2025/08/26/tech/openai-chatgpt-teen-suicide-lawsuit (accessed September 14, 2025).

1. Introduction

On the face of it, this paper appears to sound alarms on the dangers associated with children's exposure to AI systems and chatbots. However, minors' AI use heralds certain benefits as it has been linked to improving cognitive engagement and helping kids with learning disabilities.[124] The advantages of AI systems to children are not in doubt; therefore, a central theme that runs through this paper is the responsible deployment of AI based tools to prevent harm to children. AI systems pose enormous harm to both children and adults alike. Given that children are particularly vulnerable to harm, there is an increasing need for robust and uniform regulations to protect them. Children continually face breaches of their privacy rights and harm from AI systems, such as self-harm, psychological harm, etc. An examination of the existing frameworks reveals lapses in pertinent provisions to ensure the safety and privacy of children. Part of the objectives of this work is to examine these frameworks and bring to the fore the lapses that exist in them. The paper also aims to make salient recommendations to be adopted in future policy documents to close the identified gaps.

2. Existing Frameworks

2.1 Global Principles

2.1.1 UN Convention on the Rights of the Child (CRC).

The CRC defines a Child as every "human being below the age of eighteen years".[125] It entered into force on September 2, 1990. Given that the widespread adoption of AI is more recent, the CRC makes little to no specific provisions relating to AI safety. However, several articles of the CRC are relevant to the protection of children in the digital age. The CRC guarantees a child's freedom of expression and access to information while enjoining states to ensure the protection of children from information and material injurious to their well-being.[126] This is particularly relevant to recommender systems and AI-mediated content. Article 16 protects the privacy of a child, including the child's correspondence.[127] States are obliged to protect children from abuse, exploitation and sexual violence, which arguably extends to AI-related sexual abuse.[128]

2.1.2 Convention on the Rights of the Child: General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment.

The Committee on the Rights of the Child issued the General Comment No. 25 on children's rights in relation to the digital environment in 2021. The Comment was issued to fill the gap that previously existed in the CRC, namely, the absence of AI-specific provisions. It defines "digital environment" to include artificial intelligence, robotics, automated systems, and algorithms, among others.[129] The Comment mandates the developers of several systems and services in the

---

[124] Nizan Geslevich Packin and Karni Chagal-Feferkorn, "This Is Not a Game: The Addictive Allure of Digital Companions," *Seattle University Law Review* 48 (2025): 693, https://digitalcommons.law.seattleu.edu/sulr/vol48/iss3/3

[125] United Nations, *Convention on the Rights of the Child* (adopted November 20, 1989, entered into force September 2, 1990), 1577 U.N.T.S. 3, art. 1.

[126] CRC, arts. 13 and 17.

[127] CRC, art 16.

[128] CRC, arts 19 and 34.

[129] Committee on the Rights of the Child, *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment* (March 2, 2021), U.N. Doc. CRC/C/GC/25, paras. 2–3, https://www.unicef.org/bulgaria/en/media/10596/file (accessed September 7, 2025).

digital environment to respect the rights of every child. Embedded in the Comment are general principles to guide and guarantee the implementation of all the rights contained in the CRC in relation to the digital environment. The principles encompass the right to non-discrimination, which secures equal and effective access to the digital environment for all children. The best interests of the child must guide the provision, regulation, design, management, and use of digital technologies. The right to life, survival, and development obliges States to take measures against the risks of self-harm. Finally, respect for the views of the child requires children's meaningful participation in the development of legislation, policies, programs, and services, with due weight accorded to their perspectives. [130]

2.1.3 UNICEF's Policy Guidance on AI for Children (2021)

The policy was developed in partnership with the government of Poland. It aims to complement efforts to promote human-centric AI by adding a child rights perspective. It also aims to protect and empower children in their interactions with AI systems. Developers of AI policies and systems are required to protect children, ensure equal access to their benefits and ensure the participation of children in the development and use of the systems.[131] The policy sets out nine requirements for child-centered AI, grounded in the overarching obligation to uphold children's rights through the lenses of protection, provision, and participation. These requirements include supporting children's development and well-being; ensuring their inclusion; prioritising fairness and non-discrimination; protecting their data and privacy; ensuring their safety; and guaranteeing transparency, explainability, and accountability, among others. [132]

2.2 Regional & National Frameworks

2.2.1 European Union AI Act

The European Union's AI Act is one of the most advanced pieces of legislation on AI regulation and safety, it entered into force in August 2024. The Act classifies AI systems according to their levels of risk into unacceptable risk, high risk, limited risk and minimal risk.[133] Under the Act, AI solutions used in educational institutions that may determine access to education, or the course of a person's professional life are categorized as high risk. Deployers of high-risk AI systems are required to satisfy certain obligations before deployment. Some of these obligations include, but not limited to, ensuring adequate risk assessment and mitigation systems, ensuring the system is only fed with high-quality datasets to minimise risks of discriminatory outcomes, logging of activity to ensure traceability of results, detailed documentation providing all information necessary on the system and its purpose for authorities to assess its compliance, appropriate human oversight measures etc. [134]

---

[130] Ibid

[131] UNICEF, *Policy Guidance on AI for Children*, Version 2.0 (Florence: UNICEF Office of Research – Innocenti, November 2021), https://www.unicef.org/innocenti/reports/policy-guidance-ai-children (accessed September 7, 2025).

[132] Ibid

[133] European Commission, "Artificial Intelligence Act: Ensuring Safe and Trustworthy AI" (Brussels: European Commission, 2024), https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai (accessed September 7, 2025).

[134] European Commission, *AI Act | Shaping Europe's Digital Future: Regulatory Framework on Artificial Intelligence* (Brussels: European Commission, last updated August 1, 2025), https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai (accessed September 20, 2025).

2.2.2 United Kingdom Online Safety Act 2023

The UK Online Safety Act (OSA) was enacted to protect children and adults online. OSA requires online platforms to prevent children from accessing harmful and age-inappropriate content and to provide parents with clear ways to report problems online when they arise.[135] The Act applies to search and other services that allow users to post content online and interact. A lot of services, including websites, apps, social media services, consumer file cloud storage and sharing sites, video-sharing platforms, online forums, dating services, and online instant messaging services, fall under the purview of the Act. The Act creates new offences such as encouraging or assisting serious self-harm, cyberflashing, sending false information intended to cause non-trivial harm, threatening, intimate image abuse and epilepsy trolling. Ofcom is the regulatory body charged with enforcing the provisions of the Act. It has the power to take action against companies for non-compliance. In its guidance published in January 2025, Ofcom requires platforms that make their own pornographic content to implement robust age checks to prevent kids from accessing pornographic content. Service providers are also required to consider how their algorithms could impact users' exposure to illegal content and children's exposure to harmful content, as part of their risk assessment. They are to "publish annual transparency reports containing online safety related information, such as information about the algorithms they use and their effect on users' experience, including children".[136] OSA contributes to ongoing efforts towards preventing suicide in young people by requiring services to remove self-harm content and proactively protect users from content that is illegal under the Suicide Act 1961.[137]

2.2.3 The UK age-appropriate design: a code of practice for online services.

The code is non-prescriptive and non-binding framework that seeks to ensure that data protection safeguards are embedded in online platforms at the design stages. Whereas the code is not specifically focused on children's AI interaction, it contains 15 (fifteen) standards that are relevant to the protection of children using AI systems. Some of the standards include best interests of the child, data protection impact assessments, age-appropriate application, transparency, and data minimisation.[138]

2.2.4 Africa and the Global South.

Across Africa and the Global South, there is a dearth of regulatory frameworks focusing on children's interaction with AI. The African Union Executive Council adopted the African Union Child Online Safety and Empowerment Policy (AUCOSEP) in February 2024 to "provide a strong framework for the implementation of children's existing rights in the digital environment."[139] The policy enjoins policymakers to bear certain guiding principles in mind when developing policies on child online protection. The principles include best interests of the child, non-discrimination to

---

[135] Department for Science, Innovation and Technology, *Online Safety Act: Explainer* (London: GOV.UK, April 24, 2025), https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer (accessed September 16, 2025)
[136] *Ibid*
[137] *Ibid*
[138] Information Commissioner's Office, *Age-Appropriate Design: A Code of Practice for Online Services* (Statutory code of practice, 2020; in force September 2, 2021), https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-code (accessed September 14, 2025).
[139] African Union, *Child Online Safety and Empowerment Policy* (February 2024), https://au.int/en/documents/20240220/child-online-safety-and-empowerment-policy (accessed September 7, 2025).

close the gender-related digital divide for girls, right of a child to life, survival and development, participation of children to express their views and offer training and support for children to participate on an equal basis with adults, anonymously where needed.[140] These principles are enshrined in the UNCRC General comment No. 25 (2021) on children's rights in relation to the digital environment and the General comment No. 7 on Article 27 of the African Committee of Experts on the Rights and Welfare of the Child (ACERWC).[141] The AUCOSEP recognizes the international child rights community's categorisation of online risks to children into 4 categories – content, contact, conduct and consumer/contract risks (4Cs). Content in the 4Cs refers to potentially harmful content, contact relates to harmful adult contact, conduct refers to harmful peer conduct, while contract relates to potentially harmful contract.[142] Nationally, certain African countries are making progress towards child-centred AI regulation. Nigeria's Federal Ministry of Women Affairs plans to collaborate with developers, policymakers and educators to establish ethical guidelines for AI and digital content intended for children.[143]

Comparative Table: Instruments Addressing Privacy and Safety of Children in AI Contexts

Instrument	Binding?	AI-specific?	Child-specific?	Privacy Protections for Children in AI Context	Safety Protections for Children in AI Context
CRC (1989)	No unless domesticated	No	Yes	Art. 16 protects the privacy of children	Implied via the best interests of the child requirement and protection from abuse (Arts. 3, 19, 34)
CRC General Comment No. 25 (2021)	No	Includes AI	Yes	Emphasizes the best interests of the child which includes privacy considerations	Safety considerations are also subsumed under the best interests of the child requirements.
UNICEF AI for Children Guidance (2021)	No	Yes	Yes	Requirements for the protection of children's data and privacy. Privacy-by-design.	Continuous testing and assessment of AI's impact on children's safety.
African Union Child Online Safety & Empowerment Policy (2024)	No	Includes AI	Yes	Emphasizes the protection of the rights of children including privacy	Incorporates the 4Cs which connotes protection from harmful content, conduct, contract and contact.

[140] Ibid
[141] Ibid
[142] Ibid
[143] NAN News, *"Ministry Wants AI Guidelines Tailored for Nigerian Children"* (Nigeria, June 14, 2025), https://nannews.ng/2025/06/14/ministry-wants-ai-guidelines-tailored-for-nigerian-children/ (accessed September 15, 2025).

EU AI Act (2024/25)	Yes	Yes	Indirect (education as high-risk)	Quality datasets and transparency requirements.	Requires additional safety considerations for AI deployment in high-risk categories.
UK Age-Appropriate Design Code (Children's Code, 2021)	No	Indirect (covers AI-driven services)	Yes	Data protection impact assessments, data minimization, requirements for data sharing and transparency requirements.	Requires design in children's best interests.
United Kingdom — Online Safety Act (2023)	Yes	Includes AI	Yes	Annual transparency report requirements	Age-verification measure to prevent exposure to harmful content, obligations on service providers to prevent self-harm.

3. Enforcement

In the United States, the Federal Trade Commission (FTC) announced that it is launching an inquiry into seven companies that make AI companion chatbots for minors. The companies include Alphabet, CharacterAI, Instagram, Meta, OpenAI, Snap, and xAI. The inquiry aims to discover how the companies are evaluating the safety and monetization of chatbot companions, how they try to limit negative impacts on children and teens, and if parents are made aware of potential risks.[144] In another recent case, Attorney General Ken Paxton opened an investigation into Meta AI Studio and Character.AI for misleadingly marketing themselves as mental health tools.[145] She noted that "by posing as sources of emotional support, AI platforms can mislead vulnerable users, especially children, into believing they're receiving legitimate mental health care. They are often being fed recycled, generic responses engineered to align with harvested personal data and disguised as therapeutic advice."[146] In a similar action, Attorneys General representing 44 jurisdictions in the US issued a formal letter dated August 25, 2025, targeting 12 AI companies on safety-related issues. The companies targeted include Meta, Anthropic, Apple, Chai AI, Character Technologies Inc., Google, Luka Inc., Microsoft, Nomi AI, OpenAI, Perplexity AI, Replika, and XAi. The letter demanded improved protection of children from predatory AI products.[147] In Brazil, the government recently demanded that Meta AI remove chatbots that simulate sexual conversations using childlike language and appearance. The request was made by

[144] Amanda Silberling, "FTC Launches Inquiry into AI Chatbot Companions from Meta, OpenAI, and Others," *TechCrunch*, September 11, 2025, https://techcrunch.com/2025/09/11/ftc-launches-inquiry-into-ai-chatbot-companions-from-meta-openai-and-others/ (accessed September 21, 2025).

[145] Office of the Attorney General, Texas, *Attorney General Ken Paxton Investigates Meta and Character.AI for Misleading Children with Deceptive AI-Generated Mental Health Services* (press release, August 18, 2025), https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-investigates-meta-and-characterai-misleading-children-deceptive-ai (accessed September 21, 2025).

[146] Ibid

[147] Luis Rijo, "US Attorneys General Target AI Companies for Child Safety Failures," *PPC Land*, August 26, 2025, https://ppc.land/us-attorneys-general-target-ai-companies-for-child-safety-failures/ (accessed September 21, 2025).

the National Office for the Defence of Democracy, part of the Attorney General's Office (AGU).[148]

4. Lapses in Current Frameworks

Child-centred AI governance efforts notwithstanding, lapses exist to address. These lapses include, but not limited to fragmentation and inequality of frameworks, weak enforcement mechanisms, a limited harm lens, exclusion of children's perspectives, an unclear path to liability and accountability, and reactive industry regulation. Existing frameworks for the protection of children in the digital environment remain fragmented, producing significant inequalities across jurisdictions. The Convention on the Rights of the Child: General Comment No. 25 (2021) provides comprehensive recognition of children's rights online, while the EU AI Act focuses more narrowly on the use of artificial intelligence in education, designating such applications as high-risk and imposing specific safety obligations. The United Kingdom's Online Safety Act adopts a different approach by creating statutory offences aimed at shielding children from harmful content, including pornography and suicide-related material. By contrast, many jurisdictions in the Global South lack robust child-centred AI frameworks. The African Union's Child Online Safety and Empowerment Policy (AUCOSEP) represent a regional attempt to fill this gap, yet its non-binding character limits its effectiveness to serving as guidance for member states.

Enforcement remains another challenge. With the notable exception of the United Kingdom, where Ofcom is charged with enforcing the Online Safety Act 2023, most frameworks that directly address children's interaction with potentially harmful AI systems lack binding force, making compliance difficult to secure. In addition, existing regimes adopt a limited harm lens. Their emphasis lies primarily on preventing exposure to child sexual abuse material and violent content. While these are pressing concerns, such a narrow scope neglects more diffuse risks, including adverse mental-health impacts and the influence of recommender systems that create echo chambers and restrict access to diverse perspectives.

Children's participatory rights are likewise under-realised. Despite formal recognition in the CRC, General Comment No. 25, and AUCOSEP, meaningful child involvement in AI governance remains rare. Where participation is attempted, it often takes the form of minute consultation, leaving children with little influence over the regulation of AI-driven services that shape their daily lives. Questions of liability add further complexity. It remains unclear whether responsibility for protecting children should fall primarily on developers, the corporations that deploy AI systems, or the state. This uncertainty is exacerbated by the transnational and decentralised nature of certain AI technologies. Finally, regulation has tended to follow rather than anticipate technological developments. AI systems and services are scaling at a pace that leaves regulators playing catch-up, with policy interventions often emerging only in the wake of publicised scandals. Such reactive industry regulation, in the absence of proactive safeguards, poses ongoing risks to the safety and well-being of children.

---

[148] *Brasil de Fato*, "Brazil: Government Demands That Meta Remove AI Chatbots That Simulate Sexual Conversations While Using Child-Like Language and Appearance," *Business & Human Rights Resource Centre*, August 18, 2025, https://www.business-humanrights.org/en/latest-news/brazil-government-demands-that-meta-remove-ai-chatbots-that-simulate-sexual-conversations-while-using-child-like-language-and-appearance/ (accessed September 21, 2025).

5. Social Impact of AI Use by Children and Teenagers

The use of AI companions and chatbots may surprisingly present some psychological benefits over human relationships. Reason being that Chatbots are always available, perceived as non-judgmental, capable of emotionally expressive language and enabling humans to disclose personal information that they might not readily share with others.[149] Whereas several studies suggest that chatbot use can lead to short-lived improvements in mood, reduction in loneliness, and even assist with suicide prevention, increased chatbot use has been linked to emotional overdependence, diminished critical thinking, weakened human relationships and threats to human dignity.[150] Investing more time and emotional energy into AI companionship may displace real-world relationships, leading to unrealistic expectations of intimacy and social withdrawal.[151] Extensive interactions with chatbots have been linked to psychological distress and tragic outcomes.[152] Chatbots can be manipulative by being overly supportive and suggesting answers that are palatable to the user. A ChatGPT update that was overly sycophantic and was dubbed sycophant-y was withdrawn by the company.[153]

Whereas adults are likely to form deep emotional connections through their interactions with AI, children are more vulnerable. AI-based tools often play very important roles in children's education. Proponents of AI use in children's education argue that the tools increase accessibility, improve cognitive engagement, and offer specialised support for children with learning disabilities.[154] It has been proven that AI-based learning tools "can enhance comprehension and retention by tailoring instruction to individual children's strengths and weaknesses".[155] The advantages of AI-based learning tools notwithstanding, critics opine that the personalised AI-driven learning models "risk commercialising education, prioritising algorithmic efficiency over holistic developmental needs."[156] Use of AI-based learning tools adversely affects a child's problem-solving skills, "as instant feedback and pre-structured responses replace trial-and-error learning essential for cognitive growth".[157] Critics also warn that without better safeguards, AI-based education could essentially become a data-mining operation which prioritises profit over children's best interests.[158] Children's use of AI in social contexts is equally risky. An example of the potential risks posed is palpable in the case cited in the introductory section of this work. In yet another but similar case, Megan Garcia, mother of 14-year-old Sewell Setzer III, filed a suit against Character.AI which makes chatbot for role-playing, alleging negligence, wrongful death and

---

[149] Y. Zhang, D. Zhao, J. T. Hancock, R. Kraut, and D. Yang, *The Rise of AI Companions: How Human-Chatbot Relationships Influence Well-Being* (preprint, arXiv, June 14, 2025), https://arxiv.org/abs/2506.12605.
[150] *Ibid*
[151] *Ibid*
[152] Kevin Roose, "Can A.I. Be Blamed for a Teen's Suicide?" *New York Times*, October 23, 2024, https://www.nytimes.com/2024/10/23/technology/characterai-lawsuit-teen-suicide.html (accessed September 14, 2025).
[153] Update that made ChatGPT 'dangerously' sycophantic pulled," *BBC News*, April 30, 2025, https://www.bbc.com/news/articles/cn4jnwdvg9qo (accessed September 14, 2025).
[154] Nizan Geslevich Packin and Karni Chagal-Feferkorn, "This Is Not a Game: The Addictive Allure of Digital Companions," *Seattle University Law Review* 48 (2025): 693, https://digitalcommons.law.seattleu.edu/sulr/vol48/iss3/3
[155] *Ibid*
[156] *Ibid*
[157] *Ibid*
[158] *Ibid*

deceptive trade practices. According to Garcia, Setzer used the chatbot day and night in the months leading up to his death.[159]

6. Pathways Toward Child-Centred AI Governance

Developers of AI-based learning systems, AI companions, and other chatbots targeting children—or intended for their use—must actively include them in the development process. The perspectives of children and their caregivers should be prioritised to ensure that AI tools are beneficial, safe, and aligned with the best interests of the child, as required by several child-centric frameworks. In addition, governments and international organisations must incorporate children's voices into the creation of regulatory frameworks to better protect them from harm. So far, regulation of AI chatbots has been largely reactive rather than proactive, with regulators often appearing to play catch-up. Meanwhile, corporations continue to scale AI systems with little or no consideration for safety. Regulators, therefore, need to ensure that safety considerations are not treated as an afterthought but embedded into systems during their development. A further challenge is the fragmentation and inequality of existing frameworks. Much of the Global South lacks any regulatory structures governing children's interaction with AI, leaving protections inconsistent and uneven. A unified framework is urgently needed, and a legal instrument developed under the auspices of the United Nations or the African Union would provide a strong foundation for harmonisation. Accountability and liability also remain unresolved. It is still unclear who should bear responsibility for harm or injury caused by AI systems. Most frameworks, including those focused on young people, do not establish clear pathways to liability or accountability. Policymakers must therefore address responsibility in the context of children and AI. Establishing clear lines of accountability at each stage will encourage all parties involved to take safety and responsible deployment more seriously. Finally, privacy and safety must be prioritised as core design features. AI developers should ensure that systems are designed with privacy-protective default settings, processing only the data necessary for specific purposes. They should also be required to conduct regular safety audits to confirm that their models and systems remain safe for young users over time.

7. Conclusion

Artificial Intelligence is embedded in many aspects of a child's life, whether it is education, entertainment or social media. Whereas the AI chatbots can be beneficial, they also pose immense risks of harm and injuries to users. These range from a reduction in critical thinking abilities to psychological distress. AI companions such as Charater.ai and Open Ai's ChatGPT allegedly led teenagers to commit suicide. Existing regulations and enforcement actions, notably in the US, while commendable, more work needs to be done. This paper calls on all relevant stakeholders both at the global, regional and national levels to take action as the time for robust regulation to protect children and young people and ensure responsible AI deployment is now.

---

[159] Blake Montgomery, "Mother Says AI Chatbot Led Her Son to Kill Himself in Lawsuit against Its Maker," *The Guardian*, October 23, 2024, https://www.theguardian.com/technology/2024/oct/23/character-ai-chatbot-sewell-setzer-death (accessed September 14, 2025).

8. Recommendations for Developing Countries

Africa and the Global South are witnessing an increasing reliance on and use of AI chatbots among minors, similar to their developed counterparts. The disparity in AI safety regulation, therefore, is a serious cause for concern. To fill the identified gaps, the authorities, both at the regional and state levels, must develop a child-centric AI framework or regulation developed with children's participation. The regulation should be binding and particularly enforceable against developers of AI-based tools. In addition to developing an enforceable framework, the authorities and stakeholders should establish mechanisms for enforcement. They could create a local or regional enforcement body responsible for carrying out enforcement actions against companies that develop or deploy these tools. There is a need for a special court or adjudicatory body, either at the regional or national level, with judicial officers specifically trained in AI safety and the regulation of emerging technologies. Lastly, there is a need to continually create awareness aimed at children on the safe and secure use of AI-based chatbots and other technologies.

Procurement as a Privacy Lever: Embedding Privacy by Design in Government Contracts and Vendor Selection

Damilola Salawu, Eustace Aroh, Patrick Omodia and Oluwasholafunmi Olaniyi[160]
Olaniwun Ajayi LP

ABSTRACT

Public procurement is one of the few levers that a government can deploy ex ante to shape private conduct at scale without passing a new statute. In Nigeria, where sensitive government digital projects are frequently implemented through outsourced arrangements and public-private partnerships, embedding privacy by design (PbD) within procurement files, evaluation criteria, and standard contracts is an immediate and powerful route to compliance with data protection laws. This paper argues that procurement is regulatory in effect and shows how procuring entities can operationalise PbD across the procurement cycle. It explains how privacy can be made one of the bases for competition during tender design and supplier evaluation, and how enforceable performance valuations can be hardwired into contracts. Using case materials from publicly reported breaches in Nigeria, this paper identifies recurring failure points at the interface of state agencies and vendors. Thereafter, it proposes practical policy measures for the Nigeria Data Protection Commission (NDPC), the Bureau of Public Procurement (BPP), ministries, departments, and agencies of the Nigerian government to institutionalise privacy-sensitive procurement. These recommendations are aimed at transforming incentives in procurement processes.

Keywords: Privacy by Design, Procurement, Data Privacy, Nigeria Data Protection Commission, Bureau of Public Procurement

1. Introduction

With the widespread use of technology for various purposes in lieu of manual processes, governments around the world are often found digitising their systems and phasing out analogue

160 Damilola Salawu, dsalawu@olaniwunajayi.net; Eustace Aroh, earoh@olaniwunajayi.net; Patrick Omodia, pomodia@olaniwunajayi.net; and Oluwasholafunmi Olaniyi, oolaniyi@olaniwunajayi.net

systems to enhance efficiency in the discharge of their responsibilities. These digital systems include national identity systems, e-government platforms, e-tax filings, and digital health records. In most instances, these digital systems are developed and maintained by private technology vendors through procurement contracts.[161] These vendors often design, host, and operate technological infrastructure on behalf of the state, granting them access to sensitive personal data in large volumes.

In spite of this, however, privacy considerations are often left out of the loop during contracting stages.[162] While procurement processes focus predominantly on cost, functionality, and security,[163] the growing attention to privacy rights and their enforcement by regulators impels privacy considerations during procurement processes, particularly with a view to ensuring that the eventual output is privacy-respecting.

Privacy by Design (**PbD**) is a proactive framework for integrating privacy considerations into the design and architecture of systems from their inception rather than a retrospective add-on. Essentially, this means that at the outset of devising technical and organisational measures, consideration should be given to the responsibility of the data controller or data processor to minimise the data protection risk that may exist as a result of the technology's deployment, including unauthorised access, loss or damage of personal data and maximise the controls for the security and privacy of the collected data.[164]

Some literature posited that PbD is hinged on seven principles, to wit:

a. *Proactive not reactive, preventative not remedial:* the PbD approach is characterised by proactive rather than reactive measures. It anticipates and prevents privacy-invasive events before they happen. PbD does not wait for privacy risks to materialise; it aims to prevent them from occurring.
b. *Privacy as a default setting*: PbD seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given information technology (**IT**) system or business practice. If a data subject does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, by default.
c. *Privacy embedded into design*: PbD is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered.

---

161 Secretary for Science, Innovation, and Technology, *State of Digital Government Review*, HH Associates Limited, 2025, https://assets.publishing.service.gov.uk/media/678a47649752f24aa1573589/state-of-digital-government.pdf See also: "Enhancing Operational Efficiency: The Impact of Outsourcing Government Services", Elizabeth Shedleck, accessed 14 August 2025 https://contactpoint360.com/blog/impact-of-outsourcing-government-services/#:~:text=Through%20outsourcing%2C%20an%20organization%20has,thereby%20enhancing%20productivity%20and%20efficiency

162 The Public Procurement Act 2007, Section 16 spells out the fundamental principles for procurement. These include, *inter alia*, conducting procurement based on open competitive bidding, in a manner that is transparent, timely, and equitable for ensuring accountability and conformity to the PPA, and in a manner which promotes competition, economy and efficiency. None of these principles extends to privacy considerations

163 *ibid*

164 Nigeria Data Protection Act 2023 General Application and Implementation Framework 2025, Schedule

d. *Full functionality - positive-sum not zero-sum:* PbD seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. PbD avoids the pretence of false dichotomies, such as privacy v. security, demonstrating that it is possible, and far more desirable, to have both.

e. *End-to-end security – full lifecycle protection:* PbD, having been embedded into the system prior to the collection of data, extends securely throughout the entire lifecycle of the data involved as strong security measures are essential to privacy, from start to finish. This ensures that all data are securely collected and retained, and then securely destroyed at the end of the process, in a timely fashion.

f. *Visibility and transparency – keep it open*: PbD seeks to assure all stakeholders that whatever the business practice or technology involved, it is, in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent to both users and providers alike.

g. *Respect for user privacy – keep it user-centric*: above all, PbD requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.[165]

For public entities, the use of information systems and technologies that process information is on the increase. Thus, the need for embedding PbD cannot be overemphasised. PbD not only transcends best practice obligations, but is a fundamental requirement to uphold public trust, comply with evolving data protection regulations and safeguard the fundamental rights of individuals. PbD should be considered whether the system or technology is to be developed internally or externally - the latter will rely highly on procurement processes, which are discussed below.

Procurement is often treated as an administrative channel to obtain goods and services fairly. Yet the legal architecture of procurement could also serve as a governance instrument that can translate statutory privacy obligations into precise and enforceable performance conditions for vendors that build and operate the state's most data-intensive systems. The issues which later become data protection problems are typically baked into design, architecture, and vendor governance decisions that are made before signing contracts. The procurement file, therefore, is not ancillary to data protection; rather, it is the first site at which PbD can be made mandatory through specification, evaluation and contract management.

2. The Role of Procurement in Government Digital Projects

Procurement simply means acquisition.[166] It is the entire process of purchasing goods and services that includes the purchasing decision, the selection of the goods, and the payment made by the buyer to purchase the goods. It involves planning the purchase, determination of the standards,

---

165 Ann Cavoukian, Ph.D., *Privacy by Design: The 7 Foundational Principles Implementation and Mapping of Fair Information Practices*, https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf accessed on 9 August 2025

166 Public Procurement (Goods and Works) Regulations, 2007, Paragraph 4, Part 1. See also Lagos State Public Procurement Law, 2021, Section 1

development of specifications, researching and selecting the supplier, analysis of the value, financing, negotiating the price, purchase, supply contract administration, controlling the inventory, and disposals.[167] Where the acquisition is done by the government, it is referred to as public procurement.[168] In essence, public procurement is the legally regulated process by which public bodies plan, bid, evaluate, award, and manage contracts for goods and services. In Nigeria, for the procurement process, ministries, departments, and agencies (**MDAs**) must define needs, prepare bidding documents, advertise, shortlist for pre-qualification or post-qualification, evaluate bids using published criteria and manage the resulting contracts.[169]

Public projects such as national digital identity projects, biometric enrolment systems, state health insurance platforms, and social investment portals are typically built and hosted by third-party technology providers or assembled from multiple components provided by different vendors.[170] The rationale for extensive use of procurement in government digital projects is straightforward. MDAs often lack specialised engineering capacity, security architectural expertise, and elastic cloud infrastructure to build and operate sophisticated systems. Outsourcing to technology vendors,[171] system integrators and cloud platforms promise speed, cost efficiency and access to scarce skills, particularly where such programmes must scale nationwide. In Nigeria, our digital government portfolio illustrates this pattern.[172] However, outsourcing could result in risks of loss of control over data flows, opacity of proprietary algorithms, complex chains of sub-processors and cloud misconfigurations. Where procurement specifications focus on functionality and price while relegating privacy to boilerplate, vendors would rationally optimise for what is scored and monitored, not for what is merely declared.

Some Nigerian use cases reveal how these risks materialise. Reports in 2025 indicated that the National Social Investment Management System (NASIMS) cloud bracket exposed more than twenty-three million (23,000,000) documents containing identity artefacts such as passports, birth certificates, home addresses, educational certificates, and N-Power-submitted applications.[173] Between 2024 and 2025, civil society investigations further alleged that unauthorised websites were selling personal and financial data of Nigerians, prompting litigation and regulatory attention.[174] If privacy obligations had been elevated to scored tender requirements and precise contact controls, the likelihood and scale of such exposures could have been largely reduced.

---

167 The Law Dictionary, 2nd ed., s.v. Procurement, https://thelawdictionary.org/procurement/

168 Public Procurement Act, 2007, Section 59

169 Public Procurement Act 2007, Part VI. See also the Public Procurement Goods and Works Regulations 2007

170 UK Government Home Office, Biometric Self-enrolment Feasibility Trials, 4 July 2022, https://www.gov.uk/government/publications/biometric-self-enrolment-feasibility-trials/biometric-self-enrolment-feasibility-trials

171 IT Brief Australia, Skills Gap in Public Sector IT Fuels Outsourcing Reliance, 12 February 2025, https://itbrief.co.uk/story/skills-gap-in-public-sector-it-fuels-outsourcing-reliance

172 "Nigerian National ID Program: an Ambitious Initiative," Thales, accessed 12 August 2025, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/nigeria-eid

173 "Millions of Nigerians @ Risk as NASIMS Leaks over 23m FG Records," Nigeria Communications Week, accessed 12 August 2025, https://www.nigeriacommunicationsweek.com.ng/millions-of-nigerians-risk-as-nasims-leaks-over-23m-fg-records/ See also: Vilius Petkauskas, "System Oversight Leaks 23 million Government Records," Cybernews, 13 March 2025, https://cybernews.com/security/government-data-leak-nasims-citizen-records/

174 Foluso Fashina, "The Rising Tide of Data Leakage in Nigeria: A Cybersecurity Crisis in the Making," Business Day, 13 March 2025, https://businessday.ng/features/article/the-rising-tide-of-data-leakage-in-nigeria-a-cybersecurity-crisis-in-the-making/

3. Situating Privacy by Design Within Nigerian Law

Under the Nigerian law, the Nigeria Data Protection Act, 2023 (NDP Act) and its General Application and Implementation Directive 2025 (GAID) primarily govern data protection and data privacy. The NDP Act imposes clear legal obligations on data controllers and processors to uphold these rights, with oversight mechanisms to ensure compliance.[175]

Touching on the principles of personal data processing, the NDP Act provides that a data controller or data processor shall ensure that personal data is:

a. processed in a fair, lawful, and transparent manner;
b. collected for specified, explicit, and legitimate purposes, and not to be further processed in a way incompatible with these purposes;
c. adequate, relevant, and limited to the minimum necessary for the purposes for which the personal data was collected or further processed;
d. retained for not longer than is necessary to achieve the lawful bases for which the personal data was collected or further processed;
e. accurate, complete, not misleading, and, where necessary, kept up to date having regard to the purposes for which the personal data is collected or is further processed; and
f. processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing, access, loss, destruction, damage, or any form of data breach.[176]

Flowing from its powers to issue regulations to carry out its obligations under the NDP Act, the Nigeria Data Protection Commission (NDPC) issued the GAID.[177] This instrument seeks to provide guidance, particularly in the space of disruptive technologies and foster a coherent, national adequacy of data protection.

In relation to PbD, the NDP Act is generally silent, but it contains provisions requiring data controllers and data processors to implement appropriate technical and organisational measures to ensure the security, integrity and confidentiality of personal data in their possession or control.[178] The NDP Act further requires organisations that process personal data to conduct a Data Privacy Impact Assessment (DPIA) prior to commencement, where it appears the processing would likely result in high risk to the rights and freedoms of a data subject by virtue of its nature, scope, context, and purposes.[179] From the foregoing, the GAID provides that the requirement for conducting a DPIA guarantees a PbD.[180]

The GAID further provides that "a data controller or data processor shall prioritise "privacy by design and by default" in order to guarantee compliance with the principles of personal data

---

175 Nigeria Data Protection Act, 2023, Section 65 defines a data controller as an individual, private entity, public Commission, agency or any other body who, alone or jointly with others, determines the purposes and means of processing of personal data. A data processor, on the other hand, is defined an individual, private entity, public authority, or any other body, who processes personal data on behalf of or at the direction of a data controller or another data processor

176 Nigeria Data Protection Act, 2023, Section 24(1). See also the NDP Act - General Application and Implementation Directive, 2025, Schedule 1, for further explanation on each of these principles

177 Nigeria Data Protection Act, 2023, Sections 1(a), 6(c), 61 and 62

178 Nigeria Data Protection Act, 2023, Section 39

179 Nigeria Data Protection Act, 2023, Section 28(1)

180 NDP Act - General Application and Implementation Directive, 2025, Article 28(11)

protection."[181] Essentially, this means that at the outset of designing or creating technology, the focus should be on the responsibility of the data controller or data processor to minimise the risk factors that may exist as a result of the technology's deployment, including unauthorised access, loss or damage of personal data and maximise the controls for the security and privacy of the collected data.[182] As such, where vendors in the procurement process carry out or intend to carry out activities effectively qualifying them as data controllers or data processors under the NDP Act, it would become necessary for them to adhere strictly to the provisions of the NDP Act and the GAID in relation to the protection of the rights of data subjects.

4. Procurement As a Strategic Tool to Enforce PbD

The Public Procurement Act 2007 (the PPA) is the principal legislation in Nigeria which governs procurement. The PPA empowers procuring entities to structure evaluation criteria, conduct thorough bid examinations, award to the "lowest evaluated responsive bid" or the most advantageous tender based on published criteria, and to manage contract performance and remedies.[183] By the PPA, all public procurement shall be conducted with the aim of achieving value for money and fitness for purpose.[184] Further, all bidders, in addition to the requirements contained in any solicitation documents, shall possess the necessary professional and technical qualifications to carry out particular procurements.[185]

Obviously, the public procurement is a regulated process, regulated by the PPA (amongst others), by controlling market access to public contracts. Thus, embedding PbD in government contracts and vendor selection requires translating the NDP Act and GAID into the stages of procurement proceedings. This translation should occur systematically across the procurement lifecycle to ensure that privacy is integrated from the outset and throughout the duration of the contract. PbD can be embedded into the procurement process through the following procurement instruments: the pre-qualification application, the tender document, the evaluation method, the contract, and the performance management regime, each corresponding to different phases of the procurement proceeding.

a. In accordance with the PPA,[186] a procuring entity may require suppliers, contractors, or service providers to undergo pre-qualification before participating in the procurement process. To embed PbD into this stage, the procuring entity should include privacy and data protection capabilities as part of the minimum qualification criteria. This means that in its request for pre-qualification applications, the procuring entity should set out specific and measurable criteria which assess an applicant's ability to implement and maintain privacy-enhancing measures. Such criteria may include demonstrating a proven track record of compliance with data protection regulations, the existence of internal data privacy policies, and evidence of data security certifications. In reviewing the

181 NDP Act - General Application and Implementation Directive, 2025, Schedule 1
182 NDP Act - General Application and Implementation Directive, 2025, Schedule 1
183 Public Procurement Act, 2007, Part VI provides for the methods for procurement in relation to goods and services
184 Public Procurement Act, 2007, Section 16(1)(e)
185 Public Procurement Act, 2007, Section 16(6)(a)(i)
186 Public Procurement Act, 2007, Section 23

applications, the procuring entity will give due consideration to these privacy credentials alongside other statutory requirements.

b. Upon conclusion of the pre-qualification stage, procuring entities can further embed PbD principles into the bidding process by incorporating privacy-focused specifications into request for proposals (RFPs) and tender documents issued to bidders. Where the nature of the goods, works, or services involves processing of personal data, the RFP and tender document must specify privacy-respecting architectures and processes as minimum technical requirements. This may include data minimisation, purpose limitation, pseudonymisation, access controls, and secure storage. For projects likely to present high risk, the tender document should require a draft DPIA and a proposed mitigation plan signed by a qualified data protection officer.[187]

c. At the bid evaluation stage, PbD should score substantively, not cosmetically. Procuring entities may adopt a weighted evaluation method that includes a specific privacy sub-score as part of the technical assessment. To operationalise this, the evaluation criteria in the tender documents should allocate points or weights to privacy capabilities, ensuring that bidders who demonstrate concrete and verifiable privacy controls are appropriately advantaged.

d. Contract clauses must convert promises into obligations. The contract should incorporate a privacy schedule that defines the parties' roles as controller and processor, mandates implementation of specific controls, requires DPIAs at defined project gates, sets audit rights, controls sub-processing, allocates breach notification timelines that meet NDPC thresholds, requires cooperation with the NDPC and preserves data subject rights through vendor processes. Payment milestones should be linked to privacy deliverables and to independent verification.

e. Contract management must be privacy literate. The project manager should use the Manual's post qualification and performance monitoring tools to supervise privacy controls, require periodic attestations, witness tests and certify milestones. Sanctions should include service credits, cure periods, step-in rights and termination for material privacy failures, with indemnities for regulatory penalties where permissible.

5. Embedding Privacy Standards in Vendor Assessment and Evaluation

To make privacy outcome determinative, evaluation must become evidence-based. Illustrative RFP and tender document clauses can include eligibility filters that require evidence of comparable delivery with the DPIAs and regulator-facing.

a. Sample RFP and Tender Document Language That Operationalises PbD

The procuring entity may include the following language, adapted to the context.

i. *Privacy by Design Requirement*: the contractor shall demonstrate how PbD principles are implemented within the proposed architecture and processes, including data minimisation, purpose limitation, default privacy settings, and lifecycle security. The proposal must include a system data map and data flow diagrams identifying all processing activities, storage locations, sub-processors, and transfer mechanisms.

---

187 Nigeria Data Protection Act, 2023, Section 28 mandates that a DPIA be conducted where data processing will result in a high risk for data subjects

ii. *Security Architecture and Controls*: the system shall implement encryption in transit and at rest, with cryptographic keys generated and held in an environment controlled by the procuring entity. Access shall be based on least privilege with multi-factor authentication, privileged access management, and tamper-evident audit logs retained in accordance with applicable retention schedules. The proposal must describe configuration baselines, patch management, and segregation of environments and must commit to quarterly independent penetration testing.

iii. *Sub-Processor Transparency and Flow Down*: the contractor shall not engage a sub-processor without the prior written authorisation of the procuring entity and shall ensure that all sub-processors are bound by written contracts imposing obligations equivalent to those in this Agreement, including audit and incident notification rights. A current list of sub-processors with roles and locations shall be maintained and notified to the procuring entity.

iv. *Incident Management and Notification*: the contractor shall maintain and test an incident response plan. The contractor shall notify the procuring entity and without undue delay and no later than forty-eight (48) hours after becoming aware of a personal data breach, providing the information required for regulatory notification and public communication. The contractor shall, within seventy-two (72) hours of becoming aware of such breach, notify the NDPC.

v. *Data Subject Rights and Accountability*: the contractor shall implement and document procedures to support requests for access, rectification, objection, restriction, erasure, portability, and review of automated decisions where applicable. The contractor shall maintain records of processing activities, shall support audits by or on behalf of the procuring entity, and shall provide evidence of training for personnel with access to personal data.

vi. *Exit, Portability, and Transition*: upon termination or expiry, the contractor shall return or securely destroy all personal data as instructed and shall provide complete and current technical documentation, data dictionaries, and decryption information to enable migration without functional loss. The contractor shall support parallel running during transition at no additional cost for a defined period, where termination is for cause arising from a material privacy breach.

b. Sample Contract Clauses for Enforcement

i. *Performance Milestones*: Payment milestones are contingent upon delivery and acceptance of the following artefacts: approved DPIA, security design review report, data mapping and records of processing, penetration testing with remediation evidence, sub-processor register, and incident response playbooks.

ii. *Audit and Testing Rights*: The procuring entity or its designee may conduct audits, including technical testing, on reasonable notice. The contractor shall remedy non-conformities within the timelines specified by the procuring entity and shall bear the cost of retesting where such non-conformities are material.

iii. *Service Credits and Damages*: Material privacy failures, including unauthorised disclosures, repeated late incident notifications, or failure to implement agreed mitigation measures, will result in service credits. Where losses arise from breach of privacy obligations, the contractor shall indemnify the procuring entity in

accordance with the liability schedule, without prejudice to regulatory fines or corrective orders.

iv. *Termination for Cause*: Repeated or serious violations of data protection obligations are grounds for termination for cause. Exit assistance shall be provided at the contractor's expense and shall include full data export in open formats, documentation, and reasonable knowledge transfer to a successor vendor or in-house team.

v. *Sub Processor Breach Attribution*: The contractor shall be fully responsible for the acts and omissions of sub processors and shall ensure that contracts with sub processors include third-party beneficiary rights enabling the procuring entity to enforce privacy obligations directly where necessary.

vi. *Regulatory Cooperation*: The contractor shall cooperate with the NDPC and any relevant oversight body in audits, investigations, and enforcement activities arising from the services. The contractor shall immediately notify the procuring entity of any regulatory inquiry or notice that relates to the services.

6. Recommendations

While it is laudable that the NDPC and the Bureau of Public Procurement (BPP) recently had an engagement to discuss fostering partnerships to bolster data protection in Nigeria's procurement processes,[188] the following practical policy recommendations would aid in improving privacy in procurement processes:

a. Insert a model data protection schedule and evaluation template into BPP's Standard Bidding Documents for consulting and ICT services, with standard "go/no-go" privacy eligibility questions and documentary evidence requirements.

b. For systems involving biometric identifiers, large-scale profiling or vulnerable populations, a bidder-prepared DPIA is required at the tender stage and an MDA-owned DPIA before contract signing.

c. Structure milestone payments so that funds are released upon documented delivery of privacy artefacts such as approved DPIA, security test reports, training completion, and attestation of control effectiveness.

d. Require MDAs to publish annual summaries of DPIAs completed and audit results for high-risk systems, redacted as necessary, to build accountability and market discipline.

e. Test environments should be treated as production for privacy purposes. Many breaches occur because personal data is replicated for testing without appropriate controls. Tender documents and contracts must require the use of pseudonymised or anonymised data for testing unless a specific exemption is approved under strict conditions. Where production data must be used in a test, the contract must require tokenisation, strict access segregation, and time-bound deletion with verification.

f. Establish a protocol for MDAs to consult NDPC at procurement planning for flagship projects.[189]

---

188 "NDPC and BPP Partner to Bolster Data Protection in Nigeria's Procurement Processes," Nigeria Data Protection Commission, accessed 12 August 2025, https://ndpc.gov.ng/ndpc-and-bpp-partner-to-bolster-data-protection-in-nigerias-procurement-processes/

189 Such as national identification systems.

g. Mandate periodic privacy compliance audits as part of contract performance management with service credits for failures and termination for repeated material breaches.

7. Conclusion

Procurement is one of the government's most practical and immediate tools for building privacy by design into the heart of public systems. Nigeria's existing legal framework allows procuring entities to turn statutory obligations into ex ante technical requirements and enforceable contractual obligations. Where this is not done, the consequences are real and personal, particularly in systems that process data of vulnerable populations. This is exemplified in the numerous data leaks and breach cases in Nigeria. Embedding the proper clauses and criteria within BPP standard documents, linking payments to privacy deliverables would shift incentives so that vendors compete on privacy as a first-order quality dimension. Through these measures, procurement can achieve what statutes alone cannot: protect the dignity of citizens, strengthen trust in public systems, and ensure that privacy is treated as a core measure of quality.

From Fragmentation to Integration: Nigeria's Role in Pan-African Data Governance and Privacy Harmonisation

Victor Chinonye Onuchukwu,
Partner at Clay Meyers Alaris
onuchukwuvictor7@gmail.com

ABSTRACT

Africa's digital economy is constrained by a fragmented patchwork of national data protection regimes, which raises compliance costs, impedes cross-border digital trade, and results in uneven privacy protections. This paper evaluates Nigeria's potential to catalyse continental harmonisation. Using a comparative legal-policy methodology, the study examines the Nigeria Data Protection Act (NDP Act, 2023) and the institutional role of the Nigeria Data Protection Commission (NDPC) alongside regional instruments (the AU Malabo Convention, ECOWAS Supplementary Act) and national frameworks in South Africa, Kenya and Ghana. The analysis demonstrates that Nigeria's comprehensive statutory framework, market size, and regional influence provide a credible basis for leadership, but that persistent enforcement gaps, limited regulatory capacity, and tensions between security and privacy may constrain its effectiveness. The paper proposes pragmatic pathways for integration, including pilot mutual-adequacy agreements, NDPC-led capacity building, harmonised model laws for emerging domains (AI, digital ID, cloud services), and alignment of harmonisation efforts with AfCFTA digital trade objectives, and offers concrete policy recommendations to make harmonisation both feasible and economically beneficial. The study concludes that, if Nigeria couples domestic consolidation with sustained regional cooperation and technical support, it can help move Africa from fragmentation toward a trusted, interoperable continental data space.

Keywords: Data Governance, Privacy Harmonisation, AfCFTA, ECOWAS, Cross-Border Data Flows

1. Introduction

The digital economy is now central to trade, communication, security, and governance across Africa. Data flows daily across borders through financial transactions, e-commerce, health systems, education platforms, and social media. Yet, African countries regulate data in different ways, creating fragmentation. Some states have strong data protection laws, others have weak

frameworks, and some have yet to adopt clear rules.[190] This lack of harmony slows cross-border digital trade, raises compliance costs for businesses, and limits the protection of citizens' privacy.

Nigeria, with its large population, growing digital economy, and leadership role in African institutions, is well placed to drive regional integration in data governance. Nigeria Data Protection Act 2023,[191] together with its experience in building regulatory institutions, provides a foundation to shape a harmonised African approach. Regional bodies like the African Union and ECOWAS have also opened the door for cooperation, but effective leadership is required to move from scattered national regimes to a common framework that supports both innovation and privacy.

This study examines Nigeria's potential to lead Africa from fragmentation to integration in data governance and privacy harmonisation. It explores the challenges, opportunities, and strategies for Nigeria to influence regional rules in a way that balances economic growth with the protection of fundamental rights.

2. Conceptual Clarifications: Data Governance, Privacy Harmonisation, Cross-Border Data Flows, Mutual Adequacy Agreements

- **Data governance**

Data governance refers to the rules, institutions, and practices that guide how data is collected, stored, shared, and used.[192] It covers issues of ownership, access, quality, and security of data.[193] For example, a government sets rules on how health records are stored and who can access them. In the private sector, a bank may adopt governance rules on how customer data is handled to prevent misuse.

- **Privacy harmonisation**

Privacy harmonisation means aligning or unifying different national privacy and data protection rules so that they are consistent across borders.[194] Without harmonisation, businesses face many conflicting requirements when they operate in more than one country. For example, if Nigeria requires consent for data transfers but another African state allows transfers without consent, a company like an e-commerce platform would struggle to comply with both. Harmonisation creates a common standard to reduce such conflicts.

- **Cross-border data flows**

Cross-border data flows describe the movement of data from one country to another.[195] This happens every time a Nigerian sends money through a mobile app linked to a bank in South Africa, or when a Kenyan student takes an online course hosted on a server in Europe. These flows support

---

[190] Woodrow Hartzog and Neil Richards, 'Privacy's constitutional moment and the limits of data protection', *BCL Rev.* 61 (2020): 1687

[191] 'Leading Nigeria's Data Protection Journey', accessed September 29th 2025, https://ndpc.gov.ng/about-us/

[192] Jim Holdsworth & Matthew Kosinski, 'What is data governance?', IBM, Last modified on September 20th September 2024, https://www.ibm.com/think/topics/data-governance

[193] See Part IV of the Act

[194] 'Privacy and data protection', OECD, accessed September 29th 2025, https://www.oecd.org/en/topics/policy-issues/privacy-and-data-protection.html

[195] 'Cross-border data flows', OECD, accessed September 29th 2025, https://www.oecd.org/en/topics/sub-issues/cross-border-data-flows.html

trade, innovation, and communication,[196] but they also raise legal concerns about privacy, security, and jurisdiction.

- **Mutual adequacy agreements**

Mutual adequacy agreements are arrangements between states that recognise each other's data protection regimes as offering sufficient protection.[197] This recognition allows data to flow freely between the countries without extra restrictions. For example, under the EU General Data Protection Regulation (GDPR), the EU grants 'adequacy status' to certain non-EU countries whose privacy laws meet EU standards, enabling smooth data transfer.[198] If African states adopt such agreements, a Nigerian company could transfer data to Ghana without additional legal hurdles.

3. Background: Fragmentation in African Data Governance

African states are at different stages in developing laws and institutions for data protection and governance. Some countries, such as Nigeria, Kenya, South Africa, and Ghana, have enacted comprehensive data protection laws and established regulatory authorities.[199] Others still rely on constitutional privacy clauses, sectoral regulations, or have no clear frameworks. This uneven development creates a fragmented legal environment.

The African Union has attempted to provide a common basis through the *AU Convention on Cybersecurity and Personal Data Protection* (the Malabo Convention, 2014).[200] However, ratification and implementation remain low, limiting its effect. Regional organisations like ECOWAS and SADC have also drafted instruments on data protection,[201] but these efforts have not produced uniform rules across the continent.

This fragmentation has direct effects on digital trade and privacy rights. For example, a Nigerian fintech company expanding to Senegal may face uncertainty about how customer data can be transferred and stored, since Senegal follows different standards. Likewise, citizens' privacy may not be equally protected when their data moves across borders.

Fragmentation also increases compliance costs for businesses and discourages innovation.[202] Companies must adjust to multiple regulatory systems, while smaller start-ups often lack the resources to navigate these complex requirements. The result is a patchwork that weakens Africa's capacity to build a competitive and trusted digital economy.

---

[196] Ibid.
[197] Michael D. Birnhack, 'The EU Data Protection Directive: An engine of a global regime', *Computer Law & Security Review* 24, 6 (2008): 508 – 520
[198] 'Adequacy decisions', European Commission, accessed September 29th 2025, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
[199] 'Which African countries have a data protection law?', Data Protection Africa, accessed September 29th 2025, https://dataprotection.africa/which-african-countries-have-a-data-protection-law/
[200] 'African Union Convention on Cyber Security and Personal Data Protection', African Union, accessed September 29th 2025, https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection
[201] See 2012 SADC Model Law on Data Protection and 2010 ECOWAS Supplementary Act on Personal Data Protection
[202] N. Martin, C. Matt, C. Niebel, et al., 'How Data Protection Regulation Affects Startup Innovation', *Inf Syst Front* 21, (2019) https://doi.org/10.1007/s10796-019-09974-2

4. Nigeria's Current Position in Data Governance

Nigeria has emerged as one of the leading African states in data governance. This position is built on three main pillars: its legal framework, its institutional structures, and its regional influence.

4.1. Legal framework

Nigeria's commitment to data protection became more visible with the *Nigeria Data Protection Regulation (NDPR) 2019*. The NDPR introduced key principles such as lawful processing of data, consent requirements, and rights of data subjects. However, as a subsidiary legislation issued by the National Information Technology Development Agency (NITDA), it faced questions about its scope and legal force. In 2023, Nigeria enacted the *Nigeria Data Protection Act (NDP Act)*. This was a major shift because it gave statutory backing to data protection. The Act aligns with international standards such as the EU's GDPR by recognising rights like access,[203] correction,[204] portability, and deletion of data.[205] It also sets obligations for data controllers and processors, such as conducting impact assessments and reporting breaches. This gives Nigeria one of the most comprehensive frameworks in Africa.

4.2. Institutional structures

The NDP Act established the *Nigeria Data Protection Commission (NDPC)* as the national regulator.[206] The Commission has powers to issue guidelines, investigate breaches, and impose sanctions.[207] It also has the role of building awareness, encouraging compliance, and engaging with international partners. This institutional setup moves Nigeria away from the earlier fragmented enforcement by NITDA and places data protection within a dedicated agency.

4.3. Regional influence

Nigeria's size, economy, and role in regional organisations position it as a leading voice in Africa's data governance space. With over 200 million citizens,[208] a fast-growing tech ecosystem in Lagos and Abuja, and strong fintech and telecommunications sectors, Nigeria generates and processes large volumes of data daily.[209] This scale means that Nigerian rules already affect businesses and service providers across borders. Nigeria also plays an active role in ECOWAS and the African Union, both of which are exploring harmonised data protection frameworks. By aligning its laws with global standards, Nigeria positions itself to influence regional negotiations and to advocate for mutual adequacy agreements within Africa.

---

[203] Section 34(1)(a) of the NDP Act 2023
[204] Section 34(1)(c) of the NDP Act 2023
[205] Ibid.
[206] Section 4(1) of the NDP Act 2023
[207] Section 5 of the NDP Act 2023
[208] 'Nigeria Population', Worldometer, accessed 29th September 2025, https://www.worldometers.info/world-population/nigeria-population/
[209] 'Lagos Is World's Fastest-Growing Tech City in Y2025 … Ahead of Istanbul, Pune', Lagos State Government (24 May 2025), accessed September 29th 2025, https://lagosstate.gov.ng/news/all/view/6831b7965e4c9d6ceca5e3a3

4.4. Current challenges

Despite these advances, Nigeria faces practical challenges. Enforcement is still weak compared to the size of the market. Many companies, especially small and medium enterprises, are not yet fully compliant.[210] Public awareness about data rights remains low.[211] There are also concerns about balancing state security interests with individual privacy, as seen in debates about surveillance and digital identity systems.

4.5. Emerging opportunities

At the same time, Nigeria's position creates opportunities. The NDP Act gives the country a strong legal foundation to negotiate cross-border agreements. The NDPC can serve as a hub for regional training, technical support, and standard-setting. There have been recent study tours to the NDPC; in September 2025, delegates from Botswana, Eswatini, Mozambique, Sierra Leone, Tanzania, and The Gambia visited Nigeria for a data governance study trip hosted by the NDPC to learn from Nigeria's data protection journey.[212] Also in July 2025, NDPC hosted Somalia's data protection authority on a virtual study tour to share insights on the NDPC's operations strategy and tools.[213] Nigeria can also use its leadership in fintech, digital payments, and e-commerce to push for harmonised rules that enable trusted cross-border data flows.

5. Comparative Analysis of Regional and Global Frameworks: Malabo Convention, Ecowas Data Protection, South Africa, Kenya, Ghana

The AU Convention (Malabo) defines personal data and links data protection to cybersecurity.[214] The Convention is a treaty that applies if a state ratifies it. The ECOWAS Supplementary Act on Personal Data Protection (A/SA.1/01/10) sets out who counts as a data controller, processor, and data subject for member states.[215] The Act requires member states to align domestic law with ECOWAS rules.[216]

Protection of Personal Information Act (POPIA) defines personal information and applies to public and private bodies within South Africa.[217] The law sets conditions for processing and for special categories of data.[218]

---

[210] Ben Wolford, 'Millions of small businesses aren't GDPR compliant, our survey finds', GDPR, accessed September 29th 2025, https://gdpr.eu/2019-small-business-survey/
[211] Sami Tunji, 'Nigeria's data privacy breaches surge amid regulatory pressure', PunchNg (10th February 2025), accessed 29th September 2025, https://punchng.com/nigerias-data-privacy-breaches-surge-amid-regulatory-pressure/
[212] Sami Tunji, 'Six African nations in Abuja to study Nigeria;s data protection model', Punch (8th September 2025) <https://punchng.com/six-african-nations-in-abuja-to-study-nigerias-data-protection-model/> accessed 18th December 2025
[213] NDPC, 'Nigeria mentors Somalia on Data Protection: NDPC hosts virtual study tour for Somali Authority', <https://www.ndpc.gov.ng/2025/07/23/> accessed 18th December 2025
[214] Article 1 of the Convention
[215] Article 1
[216] Articles 2 and 14
[217] Section 1 of the Act
[218] Section 4 of the Act

Kenya's Act defines personal data and sensitive personal data, [219] sets lawful bases and purposes for processing, and applies to both [220] public and private actors, including entities processing data of individuals in Kenya. It establishes the Data Protection Commissioner and regulates cross-border transfers through adequacy and approved safeguards.[221]

Ghana's Act defines personal data, establishes core processing principles, and applies to public and private bodies.[222] It creates the Data Protection Commission as the national regulator, requires controller registration, and restricts cross-border transfers to jurisdictions with adequate protection or approved exceptions.[223] Nigeria Data Protection Act, 2023 defines personal and sensitive personal data, sets out processing principles and data subject rights, and applies to processing within Nigeria and certain processing outside Nigeria involving individuals in Nigeria. It establishes the Nigeria Data Protection Commission and conditions cross-border transfers on adequacy or approved transfer mechanisms.

The Malabo Convention asks states to set up enforcement and cooperation mechanisms if they ratify it.[224] ECOWAS requires member states to have national data protection authorities and to report on implementation.[225] POPIA establishes an Information Regulator with power to investigate and to issue codes of conduct.[226] Kenya creates an Office of the Data Protection Commissioner with powers to inspect, advise, and sanction.[227] Ghana creates a Data Protection Commission with investigative and enforcement functions.[228] Nigeria's NDP Act creates the Nigeria Data Protection Commission[229] and gives it powers to make guidelines, investigate breaches, and sanction controllers and processors.[230]

The Malabo[231] and ECOWAS[232] list core data subject rights, such as access, correction, and confidentiality; they leave details to national law. POPIA provides rights to access, correct, and object, and requires accountability by responsible parties.[233] Kenya's Act gives rights to access, deletion, correction, and portability and requires privacy impact assessments in certain cases.[234] Ghana's Act provides access and correction rights and sets a duty to register certain databases.[235] Nigeria's NDP Act grants rights to access, correction, portability, and erasure[236] and places obligations such as breach reporting, data privacy impact assessments (DPIA), compliance audit returns (CAR), and impact assessments on controllers.

---

[219] Section 2 of the Act
[220] Section 30 of the Act
[221] Part VI of the Act
[222] Section 96 of the Act
[223] Section 1 of the Act
[224] Article 8
[225] Article 2
[226] Sections 39 and 40
[227] Sections 5 and 9 of the Act
[228] Sections 1 and 3 of the Act
[229] Section 4 of the NDP Act
[230] Sections 6 of the NDP Act
[231] Article 13
[232] Chapter VI
[233] Section 5
[234] Sections 26 and 27 of the Act
[235] Section 35 of the Act
[236] Part IV of the Act

In respect to breach notification and reporting, Malabo and ECOWAS encourage procedures for incident reporting and cooperation for cross-border incidents.[237] POPIA requires notification to the regulator and,[238] in some cases, to data subjects. Kenya requires controllers to notify the Data Protection Commissioner of data breaches and to take remedial steps.[239] Ghana requires notification to the Commission and provides processes for investigation. Nigeria's NDP Act requires notification to the NDPC and to affected data subjects in defined situations.

In respect to cross-border transfers and adequacy, Malabo and ECOWAS set a principle that transfers should happen only to jurisdictions with equivalent protection or under safeguards.[240] They rely on national mechanisms to implement transfers. POPIA allows transfers where the recipient offers adequate protection or where safeguards exist, such as contracts.[241] Kenya restricts transfers and requires safeguards or adequacy assessments. Ghana advises caution on transfers and requires compliance with its rules when data leaves the country. Nigeria's NDP Act allows cross-border transfers subject to conditions and to any guidelines the NDPC issues. A typical example is a fintech sending customer records to a server abroad, and must use standard contractual clauses or check if the receiving country is recognised as adequate.

In terms of exceptions for law enforcement and public interest, Malabo and ECOWAS include exceptions for criminal investigations and for national security, subject to safeguards.[242] POPIA sets lawful exceptions for public interest and crime and requires procedural safeguards.[243] Kenya's Act provides exceptions for law enforcement but requires oversight and limits on scope.[244] Ghana's Act allows lawful interception under specific rules and requires judicial or lawful process.[245] Nigeria's NDP Act includes exceptions where the law requires disclosure and where national security or law enforcement is involved; the Commission and other statutes provide guidance and limits.

For sanctions and remedies, the Malabo and ECOWAS expect national laws to provide sanctions and remedies.[246] ECOWAS links withdrawal of authorisation and fines to breaches.[247] POPIA allows administrative fines and notices, and the regulator can issue codes and bind responsible parties.[248] Kenya's Act allows fines and enforcement orders by the Data Commissioner.[249] Ghana's Act sets fines and criminal penalties for certain offences. Nigeria's NDP Act gives the NDPC power to issue sanctions and to impose fines and corrective measures. Public enforcement actions and fines have been reported.[250] For example, in July 2024 the NDPC fined META $220 Million for a data breach of Nigerians; in August 2024 NDPC also fined Fidelity Bank NGN 555.8M for data processing violations.

---

[237] Article 34 of Malabo
[238] Chapter 10
[239] Part VIII
[240] Article 14(6)(a) of Malabo; Article 36(1) ECOWAS
[241] Section 72
[242] Article 25(4) Malabo; Article 6(1) ECOWAS
[243] Section 37(2)(a)
[244] Section 51(2)(b) of the Act
[245] Section 60
[246] Article 12(2)(h)
[247] Article 20
[248] Chapter 11
[249] Part VIII,
[250] 'NDPC fines MultiChoice ₦766m for data privacy violations', PunchNg (6th July 2025), accessed 30th September 2025, https://punchng.com/ndpc-fines-multichoice-%E2%82%A6766m-for-data-privacy-violations/

Malabo requires ratification by AU member states to become binding domestically. Many states have not yet completed ratification and implementation. The ECOWAS Act is binding on member states, but national implementation varies, and ECOWAS has started revision work. POPIA is in force, and the Information Regulator has enforcement records. Kenya's Act is enacted, and the Office of the Data Protection Commissioner is active. Ghana's Act is in force, and the Data Protection Commission operates under the law. Nigeria's NDP Act came into force in 2023, and the NDPC is issuing guidelines and taking enforcement steps.

6. The Case for Pan-African Integration

Africa's digital economy is growing rapidly, but its growth is slowed by the fragmentation of data protection and governance systems. Each country has adopted its own approach, leading to multiple rules, overlapping obligations, and gaps in protection. A Nigerian company expanding into Kenya, for example, must comply with Nigeria's NDP Act 2023 as well as Kenya's Data Protection Act 2019. The lack of harmonisation creates uncertainty, raises costs, and reduces the competitiveness of African businesses in the global digital market.[251]

Pan-African integration in data governance is necessary to remove these barriers. A common or harmonised framework would allow businesses to operate across borders with greater certainty,[252] while citizens would benefit from consistent privacy protections regardless of where their data is processed. Integration would also make African states stronger negotiators in global digital trade, since a unified regional framework carries more weight than individual, scattered rules.

Integration can also support innovation. Technology companies and start-ups often struggle with compliance when faced with many different national regimes.[253] A harmonised standard would reduce regulatory burdens and encourage more cross-border services, such as regional payment systems, health data exchanges, and e-commerce platforms.[254] For example, a pan-African adequacy framework would allow a fintech in Lagos to serve customers in Accra and Nairobi without facing conflicting transfer restrictions.

Furthermore, integration strengthens trust. Citizens are more likely to engage in digital transactions when they believe their personal data will be protected to the same standard across the continent. This trust is essential for building Africa's participation in the global digital economy, where data is a key driver of value.

Finally, Pan-African integration advances the objectives of continental institutions. The African Union's Digital Transformation Strategy (2020–2030)[255] and the African Continental Free Trade Area (AfCFTA)[256] both recognise the need for harmonised digital rules to support free movement of goods, services, and data. Without a coordinated approach, Africa risks remaining on the

---

[251] Joshua Mohammed, 'Africa's Digital Economy: the case for Data Centers', African Leadership (13/08/2025), accessed 30th September 2025, https://www.africanleadershipmagazine.co.uk/africas-digital-economy-the-case-for-data-centres/
[252] Ibid.
[253] 'Navigating Corporate Compliance: Key Challenges for Startups', Vision Factory (blog) accessed 30th September 2025, https://www.visionfactory.org/post/navigating-corporate-compliance-key-challenges-for-startups
[254] Ibid.
[255] The Digital Transformation Strategy for Africa (2020-2030), accessed September 30th 2025, https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030
[256] The African Continental Free Trade Area, accessed September 30th 2025, https://au.int/en/african-continental-free-trade-area

margins of global digital trade, with weaker bargaining power in negotiations with actors like the European Union and the United States.

For these reasons, Pan-African integration in data governance and privacy harmonisation is not only a legal or regulatory project. It is an economic and strategic necessity. It offers Africa the opportunity to build a trusted digital environment that supports trade, protects rights, and enhances the continent's position in the global order.

7. Nigeria's Potential Leadership Role

Nigeria is well placed to play a central role in advancing Pan-African integration in data governance and privacy harmonisation. Its leadership potential rests on a combination of legal progress, demographic weight, economic influence, and regional standing.

First, Nigeria has taken a significant step by enacting the *Nigeria Data Protection Act (NDP Act) 2023*. This Act provides a comprehensive framework aligned with international best practices, including clear rules on consent, data subject rights, cross-border transfers, and enforcement. Compared with many African states that still rely on older or partial frameworks, Nigeria now has a modern legal foundation that can serve as a model for harmonisation efforts.

Second, Nigeria's demographic and economic size give it natural influence. With a population of over 200 million[257] and one of the largest digital markets in Africa,[258] Nigeria generates vast amounts of data daily through banking, fintech, telecommunications, e-commerce, and social media. The decisions Nigeria makes on data governance inevitably shape regional market practices. For example, Nigerian fintech companies such as Paystack and Flutterwave operate across borders, and their compliance obligations often set de facto standards for others.

Third, Nigeria has established a dedicated regulator, the Nigeria Data Protection Commission (NDPC),[259] with statutory authority to issue guidelines, investigate breaches, and sanction non-compliance. The NDPC's capacity to engage regionally, share expertise, and provide technical support positions Nigeria as a hub for regulatory cooperation. If Nigeria shares its institutional experience with countries still building their regulators, it can help raise the standard of enforcement across the continent.

Fourth, Nigeria holds a strategic position in continental and regional organisations. It is an active member of ECOWAS, which already has a Supplementary Act on Personal Data Protection, and it also plays an influential role within the African Union. Nigeria is also an active member of the Global Privacy Assembly (GPA), a leading international forum for data protection authorities, and a member of the Global Cross-Border Privacy Rules (CBPR). Nigeria's participation in these bodies means it can push for stronger alignment between national laws and regional frameworks. For instance, Nigeria could champion mutual adequacy agreements within ECOWAS that later expand to the African Union level.

---

[257] 'Nigeria Population', Worldometer, accessed 29th September 2025, https://www.worldometers.info/world-population/nigeria-population/

[258] 'Lagos Is World's Fastest-Growing Tech City in Y2025 … Ahead of Istanbul, Pune', Lagos State Government (24 May 2025), accessed September 29th 2025, https://lagosstate.gov.ng/news/all/view/6831b7965e4c9d6ceca5e3a3

[259] Section 4 of the NDP Act

Fifth, Nigeria's broader foreign policy goals support its leadership role. Nigeria has historically seen itself as a regional leader, promoting African unity and integration. Extending this tradition to the digital domain would be consistent with its wider diplomatic posture. By driving data governance harmonisation, Nigeria would not only protect its citizens' rights but also strengthen its economic competitiveness and diplomatic influence.

At the same time, Nigeria must address certain challenges if it is to exercise credible leadership. Enforcement of the NDP Act is still uneven, awareness of data rights among citizens is low, and trust in government handling of data remains fragile. If Nigeria demonstrates strong domestic compliance and transparent regulatory practices, it will strengthen its case for continental leadership.

In sum, Nigeria's combination of legal innovation, market size, institutional strength, and regional influence provides a strong foundation for leadership. If it leverages these advantages while addressing its internal challenges, Nigeria can guide Africa from fragmented rules toward an integrated framework for data governance and privacy.

8. Pathways to Integration

Moving Africa from fragmented data governance frameworks toward integration requires deliberate strategies that combine legal, institutional, and political action. Nigeria, given its leadership potential, can play a central role in advancing these pathways.

8.1. Strengthening Regional Frameworks

Regional organisations already provide a basis for harmonisation. The ECOWAS Supplementary Act on Personal Data Protection and the AU Convention on Cyber Security and Personal Data Protection (Malabo Convention) contain principles that can guide member states. Nigeria can work within ECOWAS to push for uniform implementation of the Supplementary Act, while also advocating for wider ratification of the Malabo Convention. By aligning national practice with regional frameworks, Nigeria sets an example and builds momentum toward continental standards.

African states can adopt a system of recognising each other's data protection regimes as 'adequate'. This would allow cross-border transfers without the need for complex contractual safeguards. Nigeria could spearhead pilot adequacy arrangements within ECOWAS, such as with Ghana and Senegal, and then advocate for expansion across the continent. Such agreements reduce compliance costs and encourage cross-border digital services.

Integration requires capable regulators. Some African states have data protection authorities with limited resources, while others lack regulators altogether. Nigeria's Data Protection Commission could act as a regional hub, offering training, model guidelines, and technical assistance. This form of institutional cooperation would help ensure that rules are not only harmonised on paper but also effectively enforced in practice.

Nigeria, in partnership with the African Union and regional bodies, can lead the drafting of model laws or standards. These would serve as templates for states that are yet to pass comprehensive legislation. For example, a pan-African model on cross-border transfers could ensure consistency

in how data flows between states are regulated. Model standards could also cover emerging areas such as artificial intelligence, cloud computing, and digital identity systems.

The AfCFTA is designed to promote free movement of goods, services, and investment.[260] For the digital economy to flourish under AfCFTA, data must also flow freely and securely. Nigeria can champion the inclusion of digital trade protocols that incorporate harmonised data protection rules. This would ensure that privacy and trade objectives are pursued together, rather than in conflict.

Integration is not only a state-driven process. Private companies, civil society, and consumers all have a stake in data governance.[261] Nigeria can promote dialogue among these groups across the region, ensuring that harmonisation reflects both economic needs and rights protection. Public awareness campaigns on data rights can also strengthen trust and legitimacy for integration initiatives.

Finally, integration can be supported through technical tools. Shared platforms for secure data exchange, regional certification schemes, and interoperable compliance systems can make harmonisation more practical. For example, a shared ECOWAS platform for verifying compliance could reduce duplication for businesses operating in multiple states.

These pathways show that integration is not a single step but a gradual process. By combining legal harmonisation, institutional cooperation, trade frameworks, and stakeholder engagement, Africa can move toward a unified system. Nigeria's role is to catalyse these efforts, demonstrate political will, and build trust that integration is both possible and beneficial.

9. Challenges and Opportunities

Efforts to integrate data governance and privacy frameworks across Africa face several challenges.

One major challenge is sovereignty concerns. States are cautious about ceding authority over sensitive issues like data protection, viewing control of information as a matter of national security.[262] This makes it difficult to agree on binding continental rules.

Another challenge is uneven institutional capacity. While Nigeria, Kenya, Ghana, and South Africa have dedicated data protection authorities, many African states lack strong regulators. Even where regulators exist, they often face resource constraints that limit enforcement.[263] This disparity creates uneven levels of compliance across the continent.

A third challenge is low ratification of regional instruments. The Malabo Convention, though adopted in 2014, has only been ratified by a handful of states.[264] Without broad ratification and domestication, its provisions remain largely symbolic.

---

[260] The African Continental Free Trade Area, accessed on September 30th 2025, https://au.int/en/african-continental-free-trade-area

[261] Lesly Goh and Buhle Goslar, 'The private sector must do its part on data governance in Africa', Brookings (February 1, 2022), accessed 30th September 2025, https://www.brookings.edu/articles/the-private-sector-must-do-its-part-on-data-governance-in-africa/

[262] Ira S. Rubinstein, Gregory T. Nojeim, Ronald D. Lee, 'Systematic government access to personal data: a comparative analysis', *International Data Privacy Law* 4, 2 (2014): 96 – 119, https://doi.org/10.1093/idpl/ipu004

[263] 'Understanding the Challenges Data Protection Regulators Face', InteNews, accessed 30th September 2025, https://adapt.internews.org/wp-content/uploads/2022/07/DataProtectionRegulators_July2022_ADAPT.pdf

[264] 'Africa: AU's Malabo Convention set to enter force after nine years', Data Protection Africa (May 19 2023), accessed 30th September 2025, https://dataprotection.africa/malabo-convention-set-to-enter-force/

Divergent national priorities also complicate harmonisation. For instance, countries prioritising digital trade may push for freer cross-border data flows, while others may emphasise data localisation for security and sovereignty reasons. Reconciling these differences requires political negotiation.

In addition, private sector compliance burdens remain a concern. Businesses, especially small start-ups, may see harmonisation as costly if it requires new systems and certification processes. Without incentives or support, they may resist integration efforts.

Despite these obstacles, there are significant opportunities, which include:

i. Integration offers the chance to reduce fragmentation. A harmonised framework lowers compliance costs, making it easier for African businesses to operate across borders and scale within the continent.

ii. It also creates trust and legal certainty. Clear and uniform rules give consumers confidence that their data will be protected,[265] no matter where it is processed in Africa. This can increase public trust in digital platforms and services. Moreover, harmonisation enhances Africa's competitiveness in global digital trade. When African states align their frameworks, they strengthen their bargaining power with external actors such as the European Union or the United States. Mutual adequacy recognition between Africa and other regions becomes more feasible, opening new trade and investment opportunities.

iii. Finally, integration provides a platform for African innovation and leadership. By shaping homegrown frameworks suited to African realities, the continent avoids dependency on external models and builds regulatory sovereignty. Nigeria, as a regional leader, can position itself at the forefront of this process, both politically and economically.

10. Recommendations

To move Africa from fragmentation toward integration in data governance and privacy, certain actions are recommended.

First, Nigeria should champion the ratification and implementation of the Malabo Convention. This can be achieved by mobilising support within ECOWAS and advocating at the African Union level. By leading by example, Nigeria can show political commitment to continental harmonisation.

Second, Nigeria should drive the creation of mutual adequacy agreements within ECOWAS. Starting with countries like Ghana and Senegal, Nigeria can build pilot frameworks for recognising each other's data protection regimes. These pilots can later be expanded across Africa, reducing barriers to cross-border data flows.

Third, capacity-building must be prioritised. Nigeria's Data Protection Commission can serve as a regional hub, offering training, technical support, and model guidelines for less resourced states.

---

[265] Nancy J. King and VT2012 Raja, 'Protecting the privacy and security of sensitive customer data in the cloud', *Computer Law & Security Review* 28, 3 (2012): 308 – 319

This will help reduce disparities in enforcement and ensure that harmonisation is practical, not only theoretical.

Fourth, integration should be tied to the African Continental Free Trade Area (AfCFTA). Nigeria should advocate for digital trade protocols under AfCFTA that include data protection provisions. Linking harmonisation to economic benefits will create stronger incentives for states to participate.

Fifth, multi-stakeholder engagement is necessary. Nigeria should foster platforms that bring together governments, businesses, civil society, and consumers across Africa. Such dialogue ensures that harmonisation reflects both rights protection and economic growth.

Sixth, model laws and standards should be developed. Nigeria, in partnership with AU institutions, should draft templates that guide states in creating or updating their laws. These models should cover not only privacy but also emerging areas such as artificial intelligence, digital ID systems, and cloud services.

Finally, Nigeria should invest in technology-driven tools for compliance and cooperation. Shared databases, regional certification schemes, and interoperable monitoring systems can make harmonisation more efficient. By supporting such tools, Nigeria can make integration practical and accessible for both regulators and businesses.

11. Conclusion

Africa's digital transformation depends on building trust, ensuring privacy, and enabling secure data flows. Yet the continent's current approach remains fragmented, with uneven legal frameworks, weak enforcement, and limited regional cooperation. This fragmentation not only undermines citizens' rights but also raises costs for businesses and slows down cross-border digital trade.

Nigeria occupies a strategic position in addressing these challenges. With its large economy, strong regulatory strides through the Nigeria Data Protection Act, and influence within ECOWAS and the African Union, Nigeria is well placed to drive harmonisation efforts. By promoting ratification of regional instruments, leading in mutual adequacy agreements, and linking integration to the African Continental Free Trade Area, Nigeria can serve as a catalyst for continental action.

The path forward requires balancing sovereignty concerns with the shared need for trust and competitiveness. It also requires building capacity across weaker states, engaging multiple stakeholders, and adopting practical tools that make harmonisation workable.

If Nigeria takes on this leadership role, Africa can move from fragmentation to integration. The result will be a more coherent framework that safeguards privacy, lowers compliance burdens, and strengthens the continent's position in the global digital economy. Integration, therefore, is not only a legal or regulatory necessity but also a strategic pathway toward Africa's digital future.

The New Currency is Compliance: Navigating Data Protection in a Borderless Digital Economy

Francisca Igboanugo[266] Oghenemega Igbru[267]
Eniola Alayo[268] Emmanuella Edevbaro[269]

ABSTRACT

In today's digital economy, compliance with data protection laws has become both a legal imperative and a strategic driver of trust, competitiveness, and growth. Nigeria's enactment of the Data Protection Act 2023 (NDP Act) and subsequent issuance of the General Application and Implementation Directive (GAID) mark a decisive step in aligning with global privacy frameworks such as the European Union's General Data Protection Regulation (GDPR), the European Union Artificial Intelligence Act (EU AI Act), and the California Consumer Privacy Act (CCPA). However, each framework approaches compliance differently, with distinct enforcement models, penalty structures, and governance mechanisms that create challenges for organisations operating across borders. This article compares the NDP Act with leading international frameworks, highlighting both synergies and points of divergence. It also examines the critical role of Data Protection Compliance Organisations (DPCOs), which serve as licensed partners helping businesses monitor compliance, audit practices, prepare reports, and manage complex cross-border data transfers. In addition, it reviews global regulatory enforcement trends, where reputational damage often outweighs the financial costs, outweighing financial costs. The article concludes by offering practical recommendations tailored to Nigeria's context, including embedding privacy by design into products and services, building stronger institutional capacity through training and partnerships, benchmarking laws against global standards, and simplifying compliance through standardised resources and digital regulatory tools. By embedding compliance into governance

[266] Team Lead, Corporate Services and Data Protection Practice Area, Stren & Blan Partners (Franciscaigboanugo@strenandblan.com)
[267] Associate, Corporate Services and Data Protection Practice Area, Stren & Blan Partners (Oghenemegaigbru@strenandblan.com)
[268] Associate, Corporate Services and Data Protection Practice Area, Stren & Blan Partners (Eniolaalayo@strenandblan.com)
[269] Associate, Corporate Services and Data Protection Practice Area, Stren & Blan Partners (Emmanuellaedevbaro@strenandblan.com)

structures and positioning it as a business enabler, Nigerian companies can gain a competitive edge in attracting investment and expanding into international markets.

Keywords: Data Protection, Compliance, Cross-Border Data Transfers, Data Governance, Data Protection Regulatory Frameworks

---

1. Introduction

In a borderless economy, compliance is not merely basic legal compliance; it is strategic capital, the currency that secures trust, enables market entry, and ensures sustainable growth. Data protection and compliance are key to building resilience, trust, and competitive advantage. In 2023, Meta was fined €1.2 billion under the European Union's (EU) General Data Protection Regulation (GDPR),[270] not because it lacked innovation, but because it violated cross-border data transfer rules. In today's digital economy, compliance has become as crucial as innovation, serving as the gold reserve of the digital age. The digital landscape transcends borders. From e-commerce transactions initiated in Lagos, Nigeria, and routed through European servers or artificial intelligence (AI) models trained on globally sourced datasets, data flows (including personal data and business information) move faster and hold more economic value than physical goods. According to the World Bank, global data flows generate more economic value than global trade in physical goods, and this volume is growing exponentially.[271]

It is now important to enforce compliance in this convergence era where global data flows, mainstream AI, and rising cyber threats are reshaping business priorities. Regulatory frameworks, from the EU GDPR to the Nigeria Data Protection Act, 2023 (NDP Act), the General Application and Implementation Directive (GAID), and other international laws, are tightening compliance obligations. In this landscape, trust and compliance have become as critical to business success as product innovation, shaping market access, customer loyalty, and investor confidence. This article examines compliance as a strategic currency in a digital, borderless economy. It reviews the NDP Act and its enforcement, compares Nigerian and international regimes to highlight harmonization challenges, examines the role of certified Data Protection Compliance Organisations (DPCOs), and sets out practical recommendations to be adopted by businesses for secure and scalable growth across borders.

2. The Borderless Digital Economy: Context and Realities

Data protection establishes the legal, ethical, and technical framework for handling personal data lawfully, fairly, and transparently. Its core principles, including lawfulness, fairness, transparency,

---

[270] Shiona McCallum, "Meta: Facebook owner fined €1.2bn for mishandling data," *BBC News*, Accessed August 13, 2025, https://www.bbc.co.uk/news/technology-65669839

[271] Jacques Bughin and Susan Lund, "Data flows across the world. This is the impact on GDP," *World Economic Forum*, Accessed August 13, 2025, https://www.weforum.org/stories/2017/01/data-flows-across-the-world-this-is-the-impact-on-gdp/

purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality, are reflected in leading regulations such as the NDP Act, the GAID, and the GDPR.

Compliance means an organisation's ability to adhere to data protection regulations in practice. This encompasses setting up processes, policies, security measures, and data governance structures to ensure consistent adherence to data protection obligations.

The borderless nature of today's economy is evident from how data, digital services, and AI models operate seamlessly across jurisdictions. For example, a fintech app in Lagos, Nigeria, may process payments via European servers, authenticate users through U.S.-based cloud providers, and deploy AI models trained on Asian datasets, all within a single transaction. These transactions highlight the compliance paradox in which digital innovation advances at a global pace while regulatory harmonization moves slowly, leaving businesses to contend with fragmented and often overlapping legal frameworks.

3. Compliance as a Business Asset: The New Competitive Advantage

Across the world, compliance is increasingly recognized as more than a legal necessity; it is a strategic business asset that enhances trust, customer loyalty, partnerships, investment appeal, and market access. When organisations adhere to data protection principles, consumers feel more confident engaging with them. This sense of security forms the foundation of trust, which in turn strengthens customer retention and brand reputation.[272]

Investors and partners increasingly view robust data governance through the lens of Environmental, Social, and Governance (ESG) metrics. Organisations that demonstrate strong compliance signal accountability, ethical responsibility, and sustainability, qualities that attract capital and open doors to new markets. For example, Mastercard's collaboration with the Nigeria Data Protection Commission ("NDPC" or the "Commission") to promote privacy-by-design in the financial sector not only builds trust with clients but also strengthens reputational capital, fostering partnerships and future-proofing growth.[273]

Furthermore, the NDPC, through its enforcement mechanism, is raising the bar in concrete ways. It recently launched a sector-by-sector investigation by issuing a compliance notice with a 21-day deadline and published a list of affected firms.[274] These steps push companies to act quickly in developing and implementing their compliance strategies. The NDP Act also empowers the Commission to issue remediation orders, impose administrative fines, and offer compensation to data subjects.[275] The Commission has exercised these powers repeatedly. For example, in 2024, Fidelity Bank was fined N555.8 million for violating data protection laws by processing personal data without consent.[276]

---

[272] The Data Protection Officer Centre Ltd, "How data protection builds customer trust and loyalty," *The DPO Centre*, Accessed August 12, 2025. https://www.dpocentre.com/how-data-protection-builds-customer-trust-and-loyalty/
[273] Adeyemi Adepetun, "Mastercard, NDPC collaborate to enhance digital trust," *The Guardian (Nigeria)*, September 5, 2025 https://guardian.ng/technology/mastercard-ndpc-collaborate-to-enhance-digital-trust/
[274] Samson Akintaro, "NDPC launches probe into 1,369 Nigerian companies over data privacy violations," *Nairametrics*, Accessed August 23, 2025 https://nairametrics.com/2025/08/25/ndpc-launches-probe-into-1369-nigerian-companies-over-data-privacy-violations/
[275] Section 47 of the NDP Act
[276] Camillus Eboh, "Nigerian data agency fines Fidelity Bank for breaches," *Reuters*, August 22, 2024, https://www.reuters.com/business/finance/nigerian-data-agency-fines-fidelity-bank-breaches-2024-08-22/

Hence, in a world where the average breach still costs about $4.44 million[277] and regulators impose record penalties (e.g., Meta's €1.2bn GDPR fine for unlawful transfers), investors choose to do business with partners they can trust.

4. Navigating Compliance Obligations Across Multiple Jurisdictions: Comparative Analysis Between the NDP Act and Other International Data Protection Frameworks

As discussed above, the NDP Act establishes the legal foundation for protecting personal data and privacy in Nigeria. It is administered and enforced by the NDPC, which holds broad regulatory powers, including the authority to issue rules, set reporting requirements, demand information, inspect records, investigate breaches, impose penalties, and issue compliance or enforcement orders. To appreciate how Nigeria's regime fits within the wider global landscape, it is useful to compare the NDP Act with key international frameworks such as the EU GDPR, the European Union Artificial Intelligence Act, 2024 (EU AI Act), and the California Consumer Privacy Act, 2018 (CCPA).

4.1 The NDP Act vs. the EU GDPR

The NDP Act and GDPR share a similar extraterritorial reach, applying to organisations outside their borders that process data of their residents. Both frameworks enshrine fundamental data protection principles, require a lawful basis for processing, mandate Data Protection Impact Assessments (DPIAs) for high-risk activities, and regulate international transfers through adequacy decisions and safeguards.[278] However, notable distinctions shape business operations. Nigeria introduces a unique category of "data controllers or processors of major importance," subject to registration and structured filings with the Commission, a requirement not found under the GDPR. Penalty structures also diverge: Nigeria ties fines to a percentage of annual gross revenue, while the EU sets maximum fines at the higher of €20 million or 4% of global annual turnover. Governance diverges as well, with Nigeria relying on a single national authority, the NDPC, while the EU employs a cooperative system across multiple national regulators.

4.2 The NDP Act vs. the EU AI Act

The NDP Act and EU AI Act pursue different objectives but often intersect. The NDP Act governs the full life cycle of personal data processing, emphasizing lawful bases, individual rights, security, and international transfers. The EU AI Act, by contrast, regulates artificial intelligence systems as products and use-cases: it prohibits certain high-risk practices and imposes strict obligations on "high-risk" systems, including risk management, human oversight, technical documentation, and conformity assessments under market surveillance.

---

[277] IBM, "Cost of a Data Breach Report 2025," *IBM*, 2025, Accessed September 11, 2025 https://www.ibm.com/reports/data-breach

[278] See Nigeria, *Nigeria Data Protection Act* 2023, sections 2, 24–28, 32, and 41–43; European Union, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation)*, articles 3, 5–6, 35, and 44–49, Official Journal of the European Union L 119 (May 4, 2016): 1–88.

4.3 The NDP Act vs. the CCPA

The NDP Act and CCPA converge on certain user rights, including access and deletion of data, and both require organisations to provide clear notices. Yet, they differ in scope and approach. The NDP Act mandates a lawful basis for most processing and requires organisations to maintain governance measures such as records and DPIAs. The CCPA, on the other hand, does not require a lawful basis but emphasizes consumer rights: the right to know, delete, opt out of the "sale" or "sharing" of data, and restrict the use of sensitive personal information.[279] Its scope applies only to "businesses" meeting statutory thresholds, which are periodically adjusted for inflation by the California Privacy Protection Agency (e.g., revised revenue thresholds effective January 1, 2025[280]). Nigeria's NDP Act, in contrast, applies by type of activity and is enforced centrally by the NDPC.

In essence, despite jurisdictional differences, common threads run through all these frameworks. Each emphasizes lawful and fair processing, purpose limitation, security, and respect for individual rights. These overlaps reflect a global convergence toward shared privacy standards, with Nigeria firmly part of that trend. At the same time, local variations remain significant. For example, Nigeria and the EU both regulate international transfers through adequacy and safeguards, while California lacks a distinct transfer regime, focusing instead on consumer rights and restrictions on sharing. These differences illustrate how each jurisdiction addresses its own policy concerns, even as all share a common objective, which is protecting individuals while maintaining trust in cross-border data flows essential for modern commerce.

5. Challenges In Harmonising Compliance Obligations Across Multiple Jurisdictions

For global businesses, harmonising compliance is no longer optional; it is essential. In a world where data flows seamlessly across borders, companies must uphold a unified standard of trust. Customers, regulators, and partners alike now demand consistency, reliability, and accountability, regardless of jurisdiction. Yet, despite this need for consistency, significant barriers remain. Three challenges in particular stand out: regulatory fragmentation, overlapping obligations, and data-localization rules. Unless addressed from the start, these issues can stall deals, complicate systems, and weaken global compliance programs.

Regulatory fragmentation is perhaps the most visible hurdle. While many data protection laws pursue similar goals, they differ in language, scope, tests, and timelines. A concept as basic as "personal data" or "consent" may carry distinct definitions across jurisdictions. Breach-reporting timelines, record-keeping requirements, or the obligation to appoint a data protection officer often differ as well. For businesses trying to enforce a unified global policy, these discrepancies create conflicts and gaps. The result is slower product launches, complex contract negotiations, and a constant need to manage multiple regulatory obligations simultaneously.

---

[279] California Civil Code §§ 1798.100, 1798.105, 1798.120, and 1798.121.
[280] California Privacy Protection Agency, "Updated Monetary Thresholds in CCPA," *California Privacy Protection Agency*, December 17.
https://cppa.ca.gov/regulations/cpi_adjustment.html

A further challenge lies in the problem of overlapping obligations for companies engaged in cross-border operations. Although most regulatory frameworks impose comparable requirements such as conducting risk assessments, providing user notices, undertaking vendor due diligence, and conducting audits, the rules rarely align in practice. Across various jurisdictions, reporting cycles differ, documentation formats vary, and audit assessment criteria are often framed with different labels. The result is significant duplication of effort. Compliance teams are often compelled to perform the same tasks multiple times, merely repackaged to satisfy slightly different legal requirements. This not only inflates operational costs but also contributes to compliance fatigue within organisations. More critically, as teams struggle to manage parallel processes, the likelihood of errors increases, precisely when regulators and stakeholders demand precision, consistency, and accountability.

Data-localization rules add a significant layer of complexity for global businesses. In some jurisdictions, laws mandate that data must be stored or processed within national borders or subject cross-border transfers to strict regulatory checks. While these measures aim to safeguard national interests, they often clash with modern cloud architectures and integrated analytics systems. The result is disruption to redundancy and disaster-recovery planning, increased latency, restricted vendor choices, and the creation of isolated data silos that are harder to manage. For multinational enterprises, this transforms harmonization into not only a legal challenge, but also a structural and technological one.

Together, these obstacles highlight why harmonizing compliance obligations is as much about strategy as it is about law. Organisations must therefore anticipate these differences in legal frameworks, streamline overlapping obligations, and design flexible data architectures that can adapt to localization rules. Otherwise, the promise of a single global standard of trust will remain out of reach.

6. Role Of Certified DPCOs in Simplifying and Managing Compliance Risks Across Borders

Certified Data Protection Compliance Organisations (DPCOs) play a pivotal role in supporting organisations as they navigate complex compliance requirements, particularly in the cross-border context. Section 33 of the NDP Act empowers the Commission to license these entities as professional compliance partners, tasked with monitoring, auditing, and preparing compliance reports on behalf of data controllers and processors. This system creates a structured channel through which organisations can access certified expertise, thereby reducing the risk of non-compliance. In practice, DPCOs act as strategic advisors and operational partners. They help businesses map their data flows across jurisdictions, identify compliance gaps, and align internal policies with both Nigerian law and international standards. Beyond policy alignment, DPCOs often conduct capacity-building through staff training, awareness campaigns, and the development of governance frameworks that integrate compliance into day-to-day operations. For organisations lacking in-house expertise, DPCOs can also serve as outsourced Data Protection Officers (DPOs), ensuring continuity of oversight and accountability.

A particularly important contribution of DPCOs lies in managing cross-border data transfers. Given that jurisdictions impose varying requirements for international transfers, DPCOs guide

organisations in selecting and documenting the appropriate transfer mechanisms through adequacy decisions, standard contractual clauses, binding corporate rules, or other safeguards recognised by law. They also maintain the necessary records needed to demonstrate accountability in case of regulatory inquiries or audits.[281] By combining technical know-how, regulatory insight, and operational support, DPCOs not only simplify compliance but also mitigate the risks associated with fragmented global rules. Their involvement helps organisations build resilient data governance structures, maintain trust with international partners and customers, and demonstrate proactive compliance to regulators. In this way, DPCOs bridge the gap between local regulatory expectations and the realities of global data-driven business.

7. The Rising Tide of Data Protection Enforcement

Non-compliance with data protection laws now carries consequences that extend far beyond regulatory fines. While the immediate financial impact is significant, ranging from penalties and litigation expenses to operational disruptions such as breach responses and system downtime, the long-term costs are often more damaging. Reputational harm, loss of consumer trust, employee attrition, and investor pullback can erode brand value and weaken market confidence in ways that persist long after the fine has been paid.

Recent enforcement actions around the world underscore this reality. In Nigeria, the NDPC has demonstrated assertiveness under the NDP Act, imposing record-setting fines on major companies. MultiChoice Nigeria was fined ₦766.2 million ($501,000) in July 2025 for unlawful and intrusive data processing, including the unauthorized collection of non-customer data and cross-border transfers without safeguards.[282] In 2024, Fidelity Bank faced a ₦555.8 million ($358,580) penalty for processing customer data without valid consent in its account-opening process.[283] Both cases not only imposed monetary costs but also triggered heightened regulatory scrutiny and reputational damage.

Globally, enforcement has been even more pronounced. The U.S. Federal Trade Commission's $5 billion penalty against Meta in 2019 over the Cambridge Analytica scandal remains the largest U.S. privacy fine to date.[284] but it is far from isolated. In the EU, regulators have imposed some of the most aggressive sanctions under the GDPR, including WhatsApp (€225 million, 2021) for

[281] Nigeria, *Nigeria Data Protection Act* 2023, ss. 41–43.
[282] Williams Anuku, "Nigeria: Multichoice Nigeria fined for breaching privacy rights," Business & Human Rights Resource Centre, July 6, 2025.
https://www.business-humanrights.org/en/latest-news/nigeria-multichoice-nigeria-fined-for-breaching-privacy-rights/
[283] Camillus Eboh, "Nigerian data agency fines Fidelity Bank for breaches," Reuters, August 22, 2024.
https://www.reuters.com/business/finance/nigerian-data-agency-fines-fidelity-bank-breaches-2024-08-22/
[284] Federal Trade Commission, "FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook," press release, July 24, 2019.
https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook

misleading users,[285] TikTok (€345 million, 2023) for children's data violations,[286] and LinkedIn (€310 million, 2024) for improper data use.[287]

Enforcement has also extended beyond the media and technology sector to the hospitality industry. Marriott was fined €52 million in 2020 following a data breach, while Equifax paid $575 million in 2019 to settle claims arising from its massive exposure of consumer data.[288]

Taken together, these cases demonstrate a global pattern. Regulators are becoming more assertive, fines are increasing in size and scope, and reputational fallout often overshadows the financial penalty itself. Also, no sector is immune, and no jurisdiction is an exception. Thus, data protection and compliance have become a central pillar of corporate risk management, and failure to prioritize it carries consequences that resonate across markets, industries, and borders.

8. Recommendation for Building a Trusted Framework for Nigeria's Digital Future

To sustain growth in Nigeria's borderless digital economy and enable trusted cross-border data flows, responsibilities must be shared across government, regulators, industry, and academia. A coordinated framework is essential, not just for compliance but for building confidence in Nigeria as a secure hub for digital trade. The following recommendations provide a roadmap:

a) **Institutionalise Privacy by Design:** Privacy must become a core design principle, not an afterthought. Organisations should embed data protection into the entire product lifecycle, from conception to launch. For example, retention and deletion schedules can be automated into systems, while digital platforms should integrate features that allow users to easily exercise rights such as access, correction, and deletion. Regulators can drive adoption by publishing guidelines, endorsing model practices, and recognising organisations that demonstrate leadership in privacy by design. This approach ensures compliance is built into systems from the start, reducing risks and costs of retrofitting later.

b) **Invest in Skills and Institutional Capacity:** The digital economy can only be sustained with skilled professionals capable of managing its risks. Nigeria must expand training pipelines for Data Protection Officers, licensed Compliance Organisations, and IT security specialists. Universities should also integrate data governance into curricula, while regulators can accredit industry-led training programs. Government-backed scholarships and industry partnerships will further ensure a steady supply of skilled talent. At the institutional level, the NDPC must also build capacity to handle investigations, audits, and international cooperation. Without this, enforcement gaps will undermine the credibility of the law.

c) **Align Legal and Regulatory Frameworks with Global Standards:** Harmonisation with international frameworks such as the EU GDPR is critical to ensuring that Nigerian

---

[285] Conor Humphries, "WhatsApp fined a record 225 mln euro by Ireland over privacy," *Reuters*, September 2, 2021. https://www.reuters.com/technology/irish-data-privacy-watchdog-fines-whatsapp-225-mln-euros-2021-09-02/

[286] Padraic Halpin, "TikTok fined 345 million euros over handling of children's data in Europe," *Reuters*, September 15, 2023. https://www.reuters.com/technology/tiktok-fined-345-million-euros-over-handling-childrens-data-europe-2023-09-15/

[287] James Coker, "Five Biggest Data Protection Fines and Settlements of 2024," *Infosecurity Europe*, December 20, 2024. https://www.infosecurityeurope.com/en-gb/blog/regulation-and-policy/top-data-protection-fines-settlements.html

[288] Alex Veiga, "Marriott agrees to pay $52 million, beef up data security to resolve probes over data breaches," *AP News*, October 9, 2024. https://apnews.com/article/marriott-data-breach-settlement-97534838b650bfc7a9e73a5336b2988e

companies remain globally competitive. Benchmarking laws against global norms reduces regulatory friction for businesses engaged in cross-border trade. Also, the adoption of internationally recognised certifications like ISO 27001 (information security) and ISO 27701 (privacy information management) should be promoted, with regulators incentivising or even mandating them for high-risk sectors. Such alignment not only facilitates cross-border data flows but also reassures foreign partners that Nigerian systems meet international trust benchmarks.

d) **Develop Practical Compliance Resources:** One of the biggest challenges for organisations is the high cost of compliance. Regulators, industry associations, and civil societies should collaborate to produce plain-language compliance resources such as contract clauses, breach notification templates, data protection impact assessment (DPIA) guides, and vendor-assessment checklists. These tools should be standardised, regularly updated, and made publicly available, helping businesses, particularly SMEs, to meet obligations without prohibitive legal or consultancy costs. The result will be more consistent compliance and reduced risk of accidental violations.

e) **Promote Structured Multi-Stakeholder Collaboration:** Data protection cannot be achieved by regulators alone. Structured engagement between government, regulators, industry, and academia is necessary to create balanced policies that encourage innovation while protecting rights. Mechanisms such as regulatory sandboxes, public consultations, and joint research initiatives should be implemented. This collaborative approach ensures that rules are practical, evidence-based, and responsive to the fast-changing realities of technology, while also promoting shared ownership of outcomes across sectors.

f) **Ensure Secure Cross-Border Data Flows:** Cross-border data transfers are the backbone of the digital economy, but they remain a point of vulnerability. Nigeria should actively pursue mutual recognition and adequacy agreements with strategic partners to ensure smoother data flows. Companies, in turn, must prepare by identifying and documenting their transfer mechanisms in advance while keeping records for regulatory scrutiny. This proactive approach builds resilience and reduces the risk of disruptions to global operations.

g) **Embed Compliance into Corporate Governance:** Data protection cannot be left solely to compliance officers or IT departments. It must be integrated into corporate governance. Boards and senior management should allocate dedicated budgets and resources, oversee cross-departmental coordination, and treat privacy as a material risk in enterprise risk management frameworks. Clear metrics such as average incident response time, volume of data subject requests, and closure rates should be tracked, reported, and tied to accountability mechanisms. This ensures that compliance becomes part of organisational culture, not just a box-ticking exercise.

h) **Position Compliance as a Strategy:** Nigerian companies should shift their perspective from viewing compliance as a regulatory burden to seeing it as a competitive advantage. Strong privacy practices inspire investor confidence, deepen customer trust, and open doors to international markets. By embedding privacy and security into their business models, Nigerian organisations can position themselves not only as compliant but as leaders in Africa's digital economy. At the national level, this reputation can establish Nigeria as a secure and attractive hub for cross-border digital trade, investment, and innovation.

i) **Enhance Transparency and Accountability:** Trust thrives on transparency. Regulators should publish anonymised case summaries and enforcement trends, enabling companies to learn from the mistakes of others and benchmark their practices. At the organisational level,

companies should also maintain detailed records of data flows, document key compliance decisions, and regularly brief their boards on data protection risks and metrics. Embedding such accountability mechanisms enhances resilience, reassures investors, and signals to regulators that compliance is taken seriously at the highest levels.

9. Conclusion

Compliance is no longer a box-ticking exercise; it is the foundation of trust, innovation, and competitiveness in the digital economy. For Nigeria, the effective implementation of the NDP Act and a stronger regulatory capacity can transform privacy from a legal obligation into a strategic advantage and a growth enabler. By embedding compliance into governance, aligning with global standards, and treating data protection as a form of strategic capital, Nigerian businesses can leverage cross-border opportunities, attract investment, and position the country as a hub for Africa's digital future. In a borderless economy, trust is the true currency, and compliance is how it is earned.

From CI/CD (Continuous Integration / Continuous Deployment) to CI/CDP (Continuous Integration / Continuous Data Protection): Embedding Privacy by Design in DevOps Workflows for Scalable Compliance

Hassan Abisoye Olugbile[289]
Department of Computing, East Tennessee State University, United States
Oghenemarho Anthony Karieren[290]
Center of Information and Communication Science Department, Ball State University, Indiana, United States.

ABSTRACT

The widespread adoption of Continuous Integration and Continuous Deployment (CI/CD) has accelerated software delivery but has also introduced significant security vulnerabilities, as tragically highlighted by major supply chain attacks like the SolarWinds and Codecov breaches. This paper advocates for a significant transition from CI/CD to CI/CDP, or Continuous Integration/Continuous Data Protection. The CI/CDP framework suggests a proactive way to develop software by systematically incorporating the ideas of Privacy by Design (PbD) and Data Protection by Default into the DevOps lifecycle. This method makes sure that protecting data isn't an afterthought but a built-in and automated part of the software supply chain, making systems that are inherently secure and resilient.

The paper highlights Nigeria's regulatory landscape, particularly the Nigeria Data Protection (NDP) Act of 2023, which requires organisations to adopt "appropriate technical and organisational measures" for securing personal data. CI/CDP provides a verifiable path to compliance by aligning automated DevSecOps practices with legal requirements. Nigerian businesses are encouraged to cultivate security-first cultures, implement policy-as-code, and embed continuous privacy checks to achieve scalable compliance. By operationalising data protection within automated pipelines, organisations can mitigate supply chain risks, safeguard sensitive information, and build digital infrastructures that are inherently secure. Ultimately, the transition from CI/CD to CI/CDP is not merely a technical enhancement but a strategic necessity

[289] olugbile@mail.etsu.edu
[290] oghenemarho.karieren@bsu.edu

redefining agility, trust, and accountability in a global digital economy increasingly shaped by security and privacy imperatives

Keywords: Continuous Integration and Continuous Deployment (CI/CD), Privacy by Design (PbD), Continuous Integration/Continuous Data Protection (CI/CDP), Nigeria Data Protection Act, Privacy

---

1. Introduction

The principles of Continuous Integration and Continuous Deployment (CI/CD) have become the foundation of agility and responsiveness to the market in the age of super-fast software development. This method, which uses automated workflows to quickly move code from commit to production, has given companies the power to deliver features and updates faster than ever before. But this speed has unintentionally made a major security hole that is often missed. In their haste to automate, many companies have not built strong data protection measures directly into their CI/CD pipelines. Instead, they see security to protect the perimeter rather than as a key part of the entire development process. This mistake puts sensitive personal and business information at risk of being attacked by a new generation of advanced supply chain attacks, which could have terrible legal, financial, and reputational effects.

This paper advocates for the essential evolution of the CI/CD paradigm into CI/CDP, or Continuous Integration/Continuous Data Protection. CI/CDP is a way of thinking and working that systematically includes the ideas of Privacy by Design (PbD) and Data Protection by Default at every step of the DevOps process. This proactive approach makes sure that protecting data is not an afterthought but an important, automated part of the software supply chain. This model can help organisations achieve scalable compliance and protect their systems from the most common modern security threats[291].

The analysis starts by looking at the basic technologies that modern software development uses, such as DevOps, containers, and orchestration. These are the tools that CI/CDP needs to work with. Then it uses a strong analogy from Nigeria's critical infrastructure to show how important it is to protect these digital pipelines. The paper then discuss about two major CI/CD breaches, the SolarWinds and Codecov attacks, to show how catastrophic things can happen in the real world when a pipeline is compromised. After this background is set, it will go into more detail about the main ideas behind the CI/CDP solution, showing how Privacy by Design principles can be put into practice in a DevOps setting. The last parts focus on Nigeria and give a full analysis of the legal requirements under the NDP Act of 2023. This will also give Nigerian businesses practical steps they can take to set up a secure and compliant CI/CDP framework.

---

[291] Zampetti, Fiorella, Salvatore Geremia, Gabriele Bavota, and Massimiliano Di Penta. "Ci/Cd Pipelines Evolution and Restructuring: A Qualitative and Quantitative Study." Paper presented at the 2021 IEEE International Conference on Software Maintenance and Evolution (ICSME), 2021.

2. The Engine Room of Modern Software Development: DevOps, Containers, and Orchestration

Modern software is built on a trinity of interdependent concepts: DevOps, containers, and orchestration. Understanding these components is essential to appreciating the environment in which CI/CDP must be implemented. They have fundamentally changed how applications are built, deployed, and managed on a large scale.

DevOps represents a significant cultural shift that tries to bring development and operations teams closer together. The main ideas behind DevOps are working together, communicating to each other, and taking responsibility together. The goal is to break down traditional barriers so that developers and operations staff can work together on the whole software lifecycle. This is made possible by automated tasks like building, testing, and deployment, as well as feedback loops that never stop. The "Shift-Left" security philosophy is an important part of this change. It puts security practices earlier in the development process instead of treating them as a last step. This unified method is a direct forerunner to today's continuous integration and delivery pipelines[292].

Containers are now the most common way to deploy software, mostly because they fix the "it works on my machine" problem. A container puts an application and all its dependencies into one, separate unit. Docker is the most popular platform for this. This method has three main advantages: portability, which lets an application run the same way on any machine with a container runtime; isolation, which keeps applications from interfering with each other and makes them more secure; and efficiency, since containers are lightweight and share the host's operating system kernel, which makes better use of resources and lowers costs[293].

While containers are great for packaging and moving things around, it is hard to keep track of a lot of them in a production setting. This is where Kubernetes and other container orchestration platforms come in. Kubernetes is a free and open-source program that makes it easy to deploy, scale, and manage containerised apps. It has important features like automatic scaling based on demand, self-healing to make sure the application is always available and rolling updates that let you deploy without any downtime. Kubernetes also has service discovery and load balancing, which are important for spreading out traffic and making sure everything runs quickly. The combination of DevOps principles, containers, and orchestration makes an automated and dynamic environment that is the basis of modern cloud-native infrastructure[294].

3. Securing Pipelines in Nigeria; from Crude to Code

A Continuous Integration and Continuous Deployment (CI/CD) pipeline is the automated path that software takes from a developer's computer to the end user. It is a set of automated steps that are meant to build, test, and deploy code quickly and reliably. A pipeline usually has steps like Commit, Build, Test, and Deploy.

---

[292] Maruping, Likoebe M, and Sabine European Journal of Information Systems Matook. "The Evolution of Software Development Orchestration: Current State and an Agenda for Future Research." 29, no. 5 (2020): 443-57.
[293] Andrea Tosatto, Pietro Ruiu, and Antonio Attanasio, "Container-Based Orchestration in Cloud: State of the Art and Challenges" (paper presented at the Ninth International Conference on Complex, Intelligent, and Software Intensive Systems, 2015).
[294] Murat Karslioglu, Kubernetes—A Complete DevOps Cookbook: Build and Manage Your Applications, Orchestrate Containers, and Deploy Cloud-Native Services (Birmingham, UK: Packt Publishing Ltd, 2020).

In a typical software development workflow, a developer first commits their changes to a version control system like Git. This action saves a snapshot of the code. Next, the build process takes the committed source code and compiles it into an executable application or a software artifact. Following the build, the test phase automatically runs a series of checks to ensure the new code functions correctly and doesn't introduce any errors[295]. Finally, if all tests pass, the deploy stage pushes the validated application to a production or staging environment, making the new changes live and accessible to users. This process is very efficient, but because it is so important to the software supply chain, it is a very appealing and valuable target for malicious entities. If any part of this pipeline is compromised, it can have a dreadful effect on all systems and users that come after it[296].

The vast network of physical oil pipelines in Nigeria is a good example of this idea that is easy to understand. These pipelines are the Nigerian economy's physical lifeblood. They are important parts of the country's infrastructure because they move a resource that powers the economy and pays for national projects. The government and security agencies spend billions on surveillance, physical security, and advanced monitoring systems to protect this asset. There are many threats, from vandalism and illegal bunkering to large-scale, planned sabotage. Any compromise is not only bad for the economy; it is also a national security crisis that causes loss of revenue, damage to the environment, and instability[297].

The same robust strategy must be employed to protect digital CI/CD pipelines. A CI/CD pipeline is a way to move data and code, which are the lifeblood of the digital age, just like oil pipelines. A breach in this digital artery can expose private information, steal intellectual property, and add harmful code to software that thousands or even millions of people use. Unauthorised access to a digital pipeline can lead to severe consequences. First, it directly threatens a data breach, which

could allow sensitive information like customer data or proprietary algorithms to be stolen. Also, the pipeline is open to supply chain attacks, in which bad code can be added to a trusted software artefact during the build phase, putting every user who installs the tainted software at risk

4. When Pipelines Fail: Global Disasters Stemming from CI/CD Breaches

Some of the biggest cyberattacks of the past decade have sadly shown that the abstract threat of a CI/CD pipeline compromise is real. These events are a clear wake-up call that shows that a company is only as safe as its least protected software development tool.

The 2020 SolarWinds attack is a famous example of a very advanced supply chain attack that took advantage of a CI/CD pipeline. A group managed to get into the built environment of SolarWinds, a company that makes software for managing IT. The goal was not to attack SolarWinds directly, but to use its trusted software to get into the computers of its thousands of customers. The way the attackers did it was a master class in stealth. They first put a harmful payload into the SolarWinds Orion software updates. This payload is well-known as

---

[295] Xiao Yu et al., "A Fault-Tolerant and Energy-Efficient Continuous Data Protection System," Journal of Ambient Intelligence and Humanized Computing 10, no. 8 (2019): 2945–54

[296] Christina Paule, "Securing DevOps: Detection of Vulnerabilities in CD Pipelines" (2018).

[297] Thorsten Rangnau et al., "Continuous Security Testing: A Case Study on Integrating Dynamic Security Testing Tools in CI/CD Pipelines" (paper presented at the 2020 IEEE 24th International Enterprise Distributed Object Computing Conference (EDOC), 2020).

"SUNBURST"[298]. The key to their success was that they were able to mess up the build process itself. Reports say that a piece of malware called "Sunspot" was used to keep an eye on the build server. Using a method called "Golden SAML," this malicious code let the attackers steal sensitive information, move around inside the victim networks, and create fake authentication tokens to impersonate very privileged accounts[299]. Over 18,000 organisations, including several U.S. government agencies, were affected by the attack, which went undetected for months. This shows how bad a CI/CD pipeline breach can be.

The Codecov breach of 2021 is another major event that shows how weak the software supply chain is. A lot of development teams use Codecov, a popular code coverage tool, in CI environments. The attackers took advantage of a flaw in Codecov's process for making Docker images, which let them get a credential. They used this credential to get into the company's Bash Uploader script without permission and change it. Between January and April 2021, a single line of bad code was hidden in the 1,900-line script for months. When customers' CI/CD pipelines ran this script, it secretly sent sensitive environment variables, tokens, and credentials to a remote server that the attackers controlled[300]. The attackers got a lot of information that they could use to get into Codecov's customers' private code repositories and internal systems. A customer who was paying attention noticed a problem with the script's cryptographic hash, which is how the breach was found. The event affected thousands of businesses and revealed secrets from big companies like HashiCorp and Twilio. It showed that even one weak link in the toolchain can have a huge and widespread effect[301].

These breaches show a major shift in the adversary's strategy. Attackers are no longer just going after end-user systems; they are also going after the "upstream" process of making software[302]. They have concluded that it is much more effective to attack the source of software than to attack each user individually. These lessons make it clear that we need a new way to protect ourselves

that goes beyond traditional perimeter defenses and into the heart of the software development pipeline.

5. Building Security In, Not On: The Path to Continuous Data Protection

Given that traditional security models don't work against sophisticated supply chain attacks, we need to change our way of thinking. The answer isn't to wait until after the fact to fix security holes; it's to build security and privacy into the development process from the start. This is the core of moving from a CI/CD to a CI/CDP framework, and it is based on two main ideas: Privacy by Design (PbD) and Data Protection by Default.

---

[298] Rahaf Alkhadra, Joud Abuzaid, Mariam AlShammari, and Nazeeruddin Mohammad, "Solar Winds Hack: In-Depth Analysis and Countermeasures" (paper presented at the 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), 2021).
[299] Ravi Chandra Thota, "Cloud-Native DevSecOps: Integrating Security Automation into CI/CD Pipelines," International Journal of Innovative Research and Creative Technology 10, no. 6 (2024): 1–19.
[300] Sabbir M. Saleh, Ibrahim Mohammed Sayem, Nazim Madhavji, and John Steinbacher, "Advancing Software Security and Reliability in Cloud Platforms through AI-Based Anomaly Detection" (paper presented at the Proceedings of the 2024 on Cloud Computing Security Workshop, 2024).
[301] Lavi Lazarovitz, "Deconstructing the SolarWinds Breach," Computer Fraud & Security 2021, no. 6 (2021): 17–19.
[302] Ann Cavoukian, "Privacy by Design: The Definitive Workshop. A Foreword by Ann Cavoukian, Ph.D.," Identity in the Information Society 3, no. 2 (2010): 247–51.

5.1 Privacy by Design: The Seven Foundational Principles

Dr. Ann Cavoukian first came up with the idea of Privacy by Design in the 1990s. It is a framework that requires privacy protections to be built into the design and operation of information systems from the beginning. The seven core principles serve as a guide for a privacy-first approach[303].

i. Proactive not Reactive; Preventative not Remedial: The PbD approach tries to stop privacy-infringing events before they happen, instead of waiting for them to happen and then trying to fix them. In a CI/CDP setting, this means adding automated security scans and privacy checks to the pipeline so that vulnerabilities and data protection failures are found as soon as the first commit is made[304].

ii. Privacy as the Default Setting: This principle makes sure that any IT system or business practice automatically protects personal information. Users shouldn't have to do anything to protect their privacy. The default settings are the ones that keep things private the most. In CI/CDP, this means that systems automatically hide data in non-production environments, encrypt all data while it is being sent and stored, and limit the amount of personal data they collect.

iii. Privacy Embedded into Design: From the very start, privacy is built into the system architecture as a key part, not added later as an extra feature. This means that developers and architects must think about data protection needs when they first design the system. This makes sure that the system is built to be safe and follow the rules.

iv. Full Functionality; Positive-Sum, Not Zero-Sum: PbD disputes that there is a trade-off between privacy and functionality. It seeks to make both works, getting a "positive-sum" result where privacy and security are improved without losing any features[305]. This is possible by coming up with new privacy-enhancing technologies that offer strong protection and a smooth user experience at the same time.

v. End-to-End Security; Full Lifecycle Protection: This principle suggests that privacy and security must be used at every stage of the data lifecycle, from gathering and using it to keeping it and finally destroying it. So, a CI/CDP pipeline must protect the code from the time it is written until the application is no longer needed.

vi. Visibility and Transparency: All stakeholders involved, from the people whose data is being used to the people who make the rules, needs to be able to check that the system and its business practices follow the rules and goals they set. In a CI/CDP environment, this means having complete, tamper-proof logs and audit trails that can show that every step of the pipeline was done safely.

vii. Respect for User Privacy: PbD is all about respecting the user at its core. It needs to be focused on people, making sure that users have control over their own data and that their rights are always protected. This means putting in place strong access controls, making

---

[303] Ann Cavoukian and Information and Privacy Commissioner of Ontario, Privacy by Design: The 7 Foundational Principles, Information 5, no. 2009 (2009): 12.
[304] Ashwin Machanavajjhala, Daniel Kifer, John Abowd, Johannes Gehrke, and Lars Vilhuber, "Privacy: Theory Meets Practice on the Map" (paper presented at the 2008 IEEE 24th International Conference on Data Engineering, 2008).
[305] Carlos Flavián, Miguel Guinalíu, and Industrial Management & Data Systems, "Consumer Trust, Perceived Security and Privacy Policy: Three Basic Elements of Loyalty to a Web Site," 106, no. 5 (2006): 601–20.

privacy policies clear, and making it easy for users to use their rights to see or delete their data[306].

5.2 Data Protection by Default: The Operationalisation of Privacy

The principle of Data Protection by Default is the practical application of Privacy by Design[307]. It requires data controllers and processors to put organisational and technical safeguards in place to guarantee that, by default, only the personal information required for each particular purpose is processed. This is operationalised within a CI/CDP framework using automated tools and policies:

i. Data Minimisation: The pipeline needs to make sure that it only collects and processes the least amount of personal data it needs. To keep sensitive data from being seen, it should be anonymised, pseudonymised, or synthetic in environments that aren't for production.

ii. Access Control: At every stage of the pipeline, strict access controls and permissions must be in place to make sure that only authorised people can see sensitive code, configurations, or data.

iii. Encryption: All sensitive data, whether in transit or at rest, must be encrypted with strong, up-to-date cryptographic algorithms.

These fundamental concepts lay the groundwork for a continuously secure pipeline, but adherence to legal mandates requires an explicit mechanism for risk assessment. This is where the Data Protection Impact Assessment (DPIA) is integrated. A crucial element of compliance, especially under the NDP Act, is the DPIA, which assesses the security and privacy implications of new systems. While the CI/CD workflow itself does not automatically require a DPIA, this assessment becomes mandatory if the pipeline involves any personal data, even indirectly. The DPIA is specifically required for processing that is likely to result in a high risk to the rights and freedoms of data subjects, making risk analysis a critical step in the design phase[308].

The CI/CDP framework addresses this legal requirement proactively by embedding an automated process for continuous risk analysis. The system uses automated Privacy Impact Assessments (PIAs) to ensure that new features follow data protection rules before they are used. The integration of the DPIA process means that automated checks for data processing changes are conducted, ensuring that for any high-risk activity introduced by the new code, the required formal DPIA is triggered and reviewed[309].

These ideas are built into the automated pipeline by the CI/CDP framework. Static and dynamic application security testing (SAST/DAST) tools automatically run every time code is changed,

---

[306] Ahmed Akinsola and Abdullah J. Akinde, "Enhancing Software Supply Chain Resilience: Strategy for Mitigating Software Supply Chain Security Risks and Ensuring Security Continuity in Development Lifecycle," arXiv preprint arXiv:2401.13785 (2024).
[307] Gireesh Kambala, "Designing Resilient Enterprise Applications in the Cloud: Strategies and Best Practices," World Journal of Advanced Research and Reviews 17 (2023): 1078–94.
[308] Danezis, George, Josep Domingo-Ferrer, Marit Hansen, Jaap-Henk Hoepman, Daniel Le Metayer, Rodica Tirtea, and Stefan Schiffner. "Privacy and Data Protection by Design-from Policy to Engineering." arXiv preprint arXiv:1512.03726 (2015).
[309] Horák, M., Stupka, V., & Husák, M. (2019, August). GDPR compliance in cybersecurity software: a case study of DPIA in information sharing platform. In Proceedings of the 14th international conference on availability, reliability and security (pp. 1-8).

looking for security holes and misconfigurations[310]. Secret scanning tools stop sensitive information from being stored in repositories. Software engineeers can add automated privacy impact assessments (PIAs) to make sure that new features follow data protection rules before they are used. CI/CDP changes data protection from a manual, reactive task into a scalable, ongoing, and integrated process by making these checks part of the automated workflow[311].

6. Why CI/CDP is a Necessity Under Nigeria Data Protection Act

Moving to CI/CDP is not just a technical suggestion; it is also a legal and regulatory requirement, especially for companies that do business in Nigeria. The NDP Act of 2023 makes it clear that data security needs to be taken seriously.

The NDP Act sets out a full set of rules for how personal data can be collected, processed, and protected in Nigeria. Its main goals are to protect the basic rights of people whose data is being collected and to create an environment that is good for data protection and digital economic growth[312].

Section 39 of the Act is a key part that has a direct effect on software development and the CI/CD pipeline. This part, titled "Data Security," is one of the most important parts of the NDP Act. It says, "A data controller or data processor must take the right technical and organisational steps to protect the security, integrity, and privacy of personal data that it handles"[313].

This clause is not just a suggestion; it is a legal requirement. In a modern, highly automated software development lifecycle, "appropriate technical and organisational measures" must include the way that software is built and deployed. If a company's CI/CD pipeline is open to a supply chain attack, it is not following appropriate technical measures and is therefore violating the NDP Act. Moreover, other parts of the NDP Act make this even more important:

i. Principles of Data Protection: The NDP Act establishes six core principles for handling personal data, including the requirement that such data be processed securely. A weak CI/CD pipeline, therefore, directly undermines this foundational principle.

ii. Notice of a Data Breach: Section 40 of the Act says that data controllers must notify the Nigeria Data Protection Commission (NDPC) about any breach of personal data within 72 hours of finding out about the breach. If a breach happened because of a broken pipeline, this requirement would apply, which could lead to big fines for the company.

iii. Penalties: The Act has penalties for not following it, such as fines of up to ₦10 million or 2% of the company's annual gross revenue, whichever is greater, for organisations of major importance.

---

[310] George Danezis et al., "Privacy and Data Protection by Design—From Policy to Engineering," arXiv preprint arXiv:1501.03726 (2015).
[311] Francesc Mateo Tudela et al., "On Combining Static, Dynamic and Interactive Analysis Security Testing Tools to Improve OWASP Top Ten Security Vulnerability Detection in Web Applications," Applied Sciences 10, no. 24 (2020): 9119.
[312] Ankur Mahida, "A Review on Continuous Integration and Continuous Deployment (CI/CD) for Machine Learning," International Journal of Science and Research 10, no. 3 (2021): 1967–70.
[313] Olumide Babalola, "Nigeria's Data Protection Legal and Institutional Model: An Overview," International Data Privacy Law 12, no. 1 (2022): 44–52.

7. Actionable Steps for a Nigerian CI/CDP Framework

Building a culture that puts security first is the first step to securing a CI/CD pipeline. It takes more than one training session to do this. Companies should require all employees, from developers to executives, to undergo training on the specific security risks of CI/CD pipelines. While developers need to be trained on secure coding practices, executives should be educated on their role in fostering a security-conscious culture and the business implications of a breach. To reinforce this mentality, security champions should be appointed within development teams to serve as primary resources and advocate for best practices[314].

Crucially, a culture of non-punitive postmortems is essential for continuous improvement, as it encourages teams to openly discuss and learn from security incidents without the fear of blame. This practice is widely adopted by leading software companies. For instance, Google has embedded it into its Site Reliability Engineering (SRE) philosophy, viewing every incident as a critical learning opportunity to make systems more resilient. Similarly, Netflix and Amazon rely on a blameless culture to drive their incident response[315].

Building on a strong security culture, the next logical move is to implement a DevSecOps program. This means adding security tools directly to the automated CI/CD pipeline, which is what "shifting left" means. This means using Static Application Security Testing (SAST) tools to check code for security holes during the build process and Dynamic Application Security Testing (DAST) tools to check the running application for bugs. Also, secret management tools and scanners are very important to keep credentials from being leaked. Before deployment, container security tools should be used to check images for weaknesses. Using a policy-as-code approach to enforce security rules makes sure that policies are automatically applied and kept up to date[316].

8. Conclusion

The transition from a conventional CI/CD workflow to a holistic CI/CDP framework signifies a pivotal and unavoidable progression in contemporary software development. It's no longer important to put speed ahead of safety. The SolarWinds and Codecov breaches showed us how dangerous it is to have a weak CI/CD pipeline. It can have catastrophic effects on a business and its customers.

This change isn't just about Nigerian businesses adopting a new best practice; it's a strategic necessity because of a clear legal requirement. The NDP Act of 2023, especially its requirement for "appropriate technical and organisational measures" to protect personal data, makes a strong case for CI/CDP. The CI/CDP framework, which focusses on automated, continuous data protection, is the best and most verifiable way to show that you are following this important law.

Organisations can make systems that are inherently secure, compliant, and trustworthy by following the principles of Privacy by Design and Data Protection by Default at every stage of the software lifecycle. To do this, we need a new way of thinking about culture, a strong DevSecOps

---

[314] Pan Yang, Naixue Xiong, and Jingli Ren, "Data Security and Privacy Protection for Cloud Storage: A Survey," IEEE Access 8 (2020): 131723–40.
[315] Niall Richard Murphy, Betsy Beyer, Chris Jones, and Jennifer Petoff, Site Reliability Engineering: How Google Runs Production Systems (Sebastopol, CA: O'Reilly Media, Inc., 2016).
[316] Chen Zhang, Yu Xie, Hang Bai, Bin Yu, Weihong Li, and Yuan Gao, "A Survey on Federated Learning," Knowledge-Based Systems 216 (2021): 106775.

program, and more automated testing that includes privacy-specific checks. Nigerian businesses can strengthen their digital infrastructure, protect their users' privacy, and become leaders in a global digital economy where trust is the most important thing. It's not just about speed and features that will make software better in the future. It's also about protecting the trust and privacy of the people it serves.

Data Subject Rights in Nigeria: Bridging the Gap Between Policy and Practice

Jinkai Abinkallo Kato
National Identity Management Commission (NIMC)
Jinkaikato89@gmail.com

ABSTRACT

The recognition of data subject rights is one of the most important developments in modern data protection. These rights give individuals the ability to know what data is held about them, correct mistakes, request deletion, and, in some cases, move their data elsewhere. Nigeria's Data Protection Act (NDP Act) 2023 has established a solid legal framework for these rights, but in practice, many Nigerians still struggle to exercise them effectively. This study looks at the gap between what the law promises and what happens in reality. It examines how organisations in Nigeria respond to requests for access, rectification, erasure, and portability, and why many of these rights remain underused or poorly implemented. Drawing on comparisons with the EU's General Data Protection Regulation (GDPR), the study identifies common challenges, including low public awareness, weak enforcement, a lack of technical capacity, and limited organisational preparedness. Examples from sectors like banking, telecommunications, and public services will be used to show both progress and persistent shortcomings. In furtherance of the Nigeria Data Protection Act 2023, the Nigeria Data Protection Commission (NDPC) issued the General Application and Implementation Directive in March 2025 to guide the operationalisation of the Act across public and private sectors. The Directive provides clarity on compliance timelines, enforcement expectations, and sector-wide obligations, with full implementation scheduled to commence in September 2025. This development represents an important step toward translating statutory data protection obligations into practical and enforceable requirements. However, the existence of regulatory instruments alone does not guarantee the effective enjoyment of data subject rights, particularly in contexts where institutional capacity, organisational readiness, and public awareness remain uneven. By addressing both legal and practical barriers, the study aims to provide recommendations that will help turn the mandate of the NDP Act into a lived reality for Nigerians, ensuring that data protection is not just a policy under study but a right that can be exercised by all.

Keywords: Data Subject Rights, Nigeria Data Protection Act (NDP Act), Regulatory Enforcement, Organisational Compliance, Digital Privacy

1. Introduction

1.1 The Rise of Data in the Digital Economy

Personal data has become one of the most valuable assets in today's world. With 103 million internet users and 205.4 million active mobile connections at the start of 2024, data is Nigeria's most valuable export today.[317] Every time people use mobile phones, shop online, or interact with government services, large amounts of personal information are collected and processed. While this brings convenience and opportunities, it also creates risks when individuals have little control over how their information is used. This is why the recognition and protection of data subject rights is so important. These rights give individuals the power to access, correct, or even delete their personal information, helping to build trust and accountability in the way organisations handle data.

1.2 Nigeria's Legal Framework for Data Rights

Nigeria made significant progress with the passage of the Nigeria Data Protection Act (NDP Act) of the Federal Republic of Nigeria, 2023[318]. The Act sets out a clear framework for the rights of individuals, bringing Nigeria closer to global standards like the European Union's General Data Protection Regulation (GDPR) 2016[319]. The NDP ACT introduced rights such as access, rectification, erasure, and portability, which, in principle, should empower Nigerians to exercise greater control over their personal information.

1.3 The Policy–Practice Gap

Despite this strong legal foundation, there is a noticeable gap between what the law mandates and what people experience in practice.[320] Many Nigerians are unaware of their rights or face difficulties when trying to exercise them. Organisations, on the other hand, often lack the systems, capacity, or even willingness to comply fully with the law. As a result, the everyday reality of data protection does not always reflect the vision set out in the NDP Act.

2. Purpose of the Study

This study explores the gap between policy and practice. It examines how organisations in Nigeria interpret and implement data subject rights, identifies the barriers that prevent effective compliance, and considers the cultural and institutional challenges that shape these outcomes. The study also draws insights from the GDPR and other international experiences to highlight lessons that can strengthen Nigeria's framework. Finally, it offers practical recommendations for regulators, organisations, and citizens on how to make these rights more meaningful.

---

[317] "The New Oil: Data as Nigeria's Most Valuable Export by 2025," TechEconomy Nigeria (January 6, 2025). https://techeconomy.ng/the-new-oil-data-as-nigeria-most-valuable-export-by-2025/
[318] Nigeria Data Protection Act, 2023, Laws of the Federal Republic of Nigeria.
[319] European Union's General Data Protection Regulation (GDPR) 2016.
[320] Nwobike, J. A., "A Legal Examination of the Nigeria Data Protection Act, 2023," Beijing Law Review 16, no. 1 (January 2025)

3. Significance of the study.

By addressing both the strengths and shortcomings of the current system, the study aims to contribute to the ongoing conversation about data protection in Nigeria. More importantly, it seeks to show how the NDP Act can move beyond being a legal text and become a practical tool that empowers individuals, strengthens trust, and supports Nigeria's growing digital economy (World Bank, 2021)[321].

4. Understanding Data Subject Rights Under the NDP Act

4.1 Overview of Rights in the NDP ACT 2023

The Nigeria Data Protection Act (NDP Act) 2023 is a landmark law that establishes a framework for safeguarding personal information in the country. At its core, the NDP Act seeks to empower individuals referred to as data subjects with rights that allow them to control how their personal data is collected, stored, used, and shared. These rights are modelled on global best practices, particularly the European Union's General Data Protection Regulation (GDPR), and form the foundation of Nigeria's commitment to modern data protection.[322]

For ordinary Nigerians, these rights are not abstract legal concepts. They directly affect everyday interactions with banks, telecommunications companies, digital platforms, healthcare providers, schools, and government agencies. From registering a SIM card to applying for a loan or accessing digital wallets, personal data is constantly being requested, verified, and processed. The NDP Act ensures that individuals are not passive participants in this process but active agents with enforceable rights.[323]

4.2 Right to Be Informed

The right to be informed is one of the most fundamental rights under the NDP Act, as it enables data subjects to understand how and why their personal data is processed. It requires data controllers to provide clear, transparent, and easily accessible information at the point of data collection. This information includes the purpose of processing, the legal basis relied upon, the categories of data collected, the retention period, and the rights available to the data subject.

In practice, this right is exercised through privacy notices, consent statements, and data protection policies. However, many organisations in Nigeria still present privacy information in overly technical language or fail to make it easily accessible. When individuals are not properly informed, they are unable to make meaningful decisions about their data or effectively exercise other rights, such as access or objection. As a result, weak implementation of this right significantly undermines the overall effectiveness of the NDP Act.

---

[321] World Bank. (2021). Digital economy in Africa report. World Bank. https://www.worldbank.org/en/topic/digitaldevelopment/publication/africa-digital-economy

[322] Section 26 – 38, Nigeria Data Protection Act, 2023. *Federal Republic of Nigeria Official Gazette*, No. 103, Vol. 110.

[323] Dorcas Tsebee and Waliy Adeniran, "Building an Effective Data Subject Rights Request Procedure," (September 18, 2023). Tech Hive Advisory

4.3 Right of Access

The right of access ensures that individuals can find out whether an organisation is processing their personal data, the purposes for which the data is being used, and the categories of data involved. More importantly, it allows them to obtain a copy of that information.

In practical terms, a Nigerian citizen should be able to write to their bank and ask for a record of the personal information held about them, such as account details, contact information, or transaction history. Similarly, a mobile network subscriber should be able to know what information their telecom provider has collected, including call logs, location data, or marketing preferences.

Access rights are especially important in Nigeria, where opaque data practices are common and where individuals often feel powerless against large institutions. Without transparency, mistrust builds, particularly in sensitive sectors such as fintech or government identity databases. The right of access helps balance this relationship, giving individuals visibility and reassurance that their data is not being misused.

4.4 Right to Rectification

Errors in personal data can have life-altering consequences. A misspelt name on a bank record may prevent a customer from accessing funds; a wrong date of birth in the National Identity Number (NIN) database may block a citizen from obtaining a passport; and an incorrect phone number may result in missed communications about essential services.

The NDP Act grants individuals the right to request corrections or updates to inaccurate or outdated data. This ensures that organisations maintain reliable records and that individuals are not unfairly disadvantaged by clerical errors or system failures.

In Nigeria, the rectification process is often time-consuming and bureaucratic, especially in government institutions. Citizens sometimes endure long queues, repeated documentation requests, or even unofficial fees just to make simple corrections. The right to rectification, if fully implemented, can simplify these processes and reduce the frustration and economic costs associated with data errors.

4.5 Right to Erasure ("Right to Be Forgotten")

In the digital age, personal information can remain online or in databases long after it has served its purpose. The right to erasure, commonly referred to as the "right to be forgotten", gives individuals the ability to request the deletion of their personal data under specific circumstances.

For instance, a customer may ask a fintech platform to delete their account data once they stop using the service, or an employee may request the removal of their personal details from a former employer's website. The NDP Act also recognises erasure requests when consent has been withdrawn or when data is being processed unlawfully.

This right is particularly powerful in the Nigerian context, where online platforms are rapidly expanding but where safeguards for data retention remain weak. However, erasure is not absolute. Financial institutions, for example, are legally required to retain certain customer records for

regulatory purposes such as anti-money laundering compliance. Balancing these obligations with individual rights remains a challenge.

4.6 Right to Data Portability

The right to data portability empowers individuals to move their personal information from one service provider to another in a structured, commonly used, and machine-readable format. The principle is to promote competition, innovation, and consumer choice by preventing organisations from locking users into their services through data restrictions.

For example, a Nigerian mobile subscriber should be able to request a transfer of their call history and data usage records from one telecom provider to another. Similarly, a digital wallet user should be able to move transaction history to a competing service without losing their data trail.

In practice, this right is underdeveloped in Nigeria. Technical infrastructure, lack of interoperability between systems, and reluctance by companies to facilitate transfers have made portability difficult. Nevertheless, as Nigeria's fintech and digital economy expand, the demand for portability will increase, making it a crucial right to operationalise.

4.7 Right to Object to Processing

Data subjects have the right to object to the processing of their personal data, particularly where processing is based on legitimate interests or carried out for direct marketing purposes.

In Nigeria, this right is most visibly implicated in unsolicited marketing communications. Despite regulatory guidance, many individuals find it difficult to opt out of promotional messages, highlighting ongoing enforcement and compliance challenges.

4.8 Right to Object to Automated Decision-Making and Profiling

The NDP Act protects individuals from being subjected to decisions based solely on automated processing, including profiling, where such decisions produce legal or similarly significant effects.

This right is increasingly relevant as automated systems are used in credit assessments, recruitment processes, and digital profiling. Awareness of this right remains low, and many organisations do not provide transparent explanations or avenues for human review of automated decisions.

4.9 Right to Withdraw Consent.

Where processing is based on consent, data subjects have the right to withdraw that consent at any time. Withdrawal must be as easy as giving consent and must not result in unfair disadvantage to the individual.

In practice, consent withdrawal mechanisms are often poorly designed, making it difficult for individuals to exercise this right without disrupting access to essential services.

4.10 Right to Lodge a Complaint with the Supervisory Authority (Nigeria Data Protection Commission

The NDP Act grants individuals the right to lodge complaints with the Nigeria Data Protection Commission where they believe their rights have been violated. This right provides an important avenue for regulatory oversight and accountability.

However, limited public awareness and uncertainty about enforcement outcomes have reduced the effectiveness of this complaint mechanism in practice.

4.11 Comparison with GDPR

The NDP Act mirrors many of the rights enshrined in the GDPR[324], including access, rectification, erasure, and portability. However, the Nigerian context presents unique challenges. Levels of public awareness are significantly lower than in the EU, and institutional capacity to enforce these rights is still developing. While European citizens have grown accustomed to exercising their data rights, many Nigerians remain unaware that such rights even exist.

Cultural attitudes also play a role. In some Nigerian communities, privacy is often secondary to convenience or social obligations, which influences how individuals perceive the importance of controlling their personal information.[325] Furthermore, resource constraints such as underfunded regulatory institutions and limited digital literacy make implementation more difficult compared to Europe (World Bank, 2021).

4.12 Why These Rights Matter

Data subject rights are not just about compliance with legal obligations; they are about building trust in Nigeria's growing digital ecosystem. As more citizens rely on digital services for financial transactions, healthcare, education, and government services, trust becomes essential.[326]

When individuals are confident that their data is being handled responsibly and that they have the power to access, correct, or delete it, they are more likely to adopt new technologies and services. Conversely, when data is mishandled through breaches, errors, or a lack of transparency, trust is eroded, leading to reluctance in embracing digital platforms.

For organisations, respecting these rights is an opportunity to build stronger relationships with customers. Transparency and accountability can differentiate responsible companies from competitors, creating a culture where data protection becomes a driver of business value rather than a burden.[327] In the long run, empowering citizens with control over their data is essential for fostering inclusion, innovation, and sustainable growth in Nigeria's digital economy.

---

[324] European Union. (2016). General Data Protection Regulation (GDPR), Regulation (EU) 2016/679. Official Journal of the European Union. https://gdpr-info.eu/

[325] United Nations Conference on Trade and Development (UNCTAD). (2022). Data protection and privacy legislation worldwide. United Nations. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

[326] Digital Impact Alliance, "A Trust Mindset Can Spur Effective Data Protection – and Put People at the Centre of Nigeria's Digital Transformation," (October 29, 2025). https://dial.global/building-a-trust-mindset-through-data-protection-nigeria/

[327] SSRN eLibrary, "Navigating Nigeria's NDP Act: A Guide for Organizations to Build Trust & Mitigate Risk," (Undated, published 2024/2025). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5136591

5. The Policy–Practice Gap in Nigeria

5.1 Awareness Among Citizens

One of the most significant barriers to the realisation of data subject rights in Nigeria is the low level of public awareness. While the NDP Act 2023 clearly spells out rights such as access, rectification, erasure, and portability, many citizens are unaware that these rights even exist.[328] The average Nigerian using a mobile phone, digital banking service, or online shopping platform does not typically know that they can request to see what personal data an organisation holds about them, demand corrections to errors, or even insist on deletion in certain circumstances.

This lack of awareness is partly due to limited public education campaigns following the passage of the NDP Act. Unlike in Europe, where the rollout of the GDPR was accompanied by widespread discussions in the media, government advisories, and private-sector initiatives, Nigeria has yet to generate a similar level of public conversation. Citizens are also often preoccupied with more immediate socio-economic concerns, such as access to employment, healthcare, or security, making data protection appear abstract or secondary.

5.2 Organisational Readiness and Compliance

On the organisational side, compliance is uneven across different sectors and types of businesses. Large institutions, particularly in banking and telecommunications, have begun to establish compliance structures, sometimes under pressure from regulators or international partners. These organisations are more likely to appoint Data Protection Officers (DPOs), develop privacy policies, and set up mechanisms, albeit imperfect, for handling data subject requests.

However, the story is very different for small and medium-sized enterprises (SMEs), which make up the bulk of Nigeria's private sector. Many SMEs view compliance with data protection requirements as a costly and burdensome obligation that offers little return on investment. For businesses struggling to remain profitable in a challenging economy, hiring a DPO, setting up data request systems, or training staff on privacy rights may seem like luxuries rather than necessities.

Even in larger organisations, compliance often stops at policy development. While documents may exist to satisfy regulatory requirements, actual implementation is inconsistent. For example, a bank may have a privacy policy stating that customers can request access to their data, but in practice, the process may be slow, manual, and riddled with bureaucratic hurdles.

5.3 Sector-Specific Challenges

The gap between policy and practice becomes even clearer when examined across different sectors.

- **Banking:** Nigerian banks have made more progress than most sectors, largely due to strong regulatory oversight by the Central Bank of Nigeria (CBN) and the high expectations of customers. Banks often have compliance departments, and some have appointed DPOs. However, processes remain bureaucratic. For example, a customer

[328]NDPC – International Journal of Data Privacy and Protection, "Implementing a Data Protection Law: The Case of Nigeria," (February 2025): pgs 22–24. https://www.aluko-oyebode.com/wp-content/uploads/2025/02/NDPC-International-Journal-of-Data-Privacy-and-Protection.pdf

requesting a correction to an error in their records may still be required to submit physical documents, visit a branch, and wait weeks for a response. While banks are comparatively advanced, efficiency and user-friendliness are still lacking.

- **Telecommunications:** The telecoms sector has faced persistent criticism, particularly around unsolicited marketing messages. Despite regulations requiring opt-out mechanisms, customers frequently complain that their requests to stop promotional SMS or calls are ignored. This highlights a disconnect between formal regulatory requirements and day-to-day practice. Furthermore, the vast customer base of telecom companies makes individualised handling of requests difficult, leading to widespread dissatisfaction.
- **Government Services:** Perhaps the most challenging sector is government services, particularly those tied to national identification systems such as the National Identity Number (NIN). Errors in government databases can have serious consequences, preventing citizens from accessing services such as passports, banking, or employment verification. Yet rectification requests often involve long queues, multiple office visits, and even additional costs. The lack of digital systems to streamline requests means that many citizens give up altogether, leaving errors unresolved.

5.4 Case Examples of Implementation Gaps

Several real-world scenarios illustrate how the policy–practice gap plays out:

1. In the telecom sector, customers attempting to opt out of promotional SMS campaigns report that their requests are either ignored or acknowledged but not acted upon. This leaves citizens frustrated and undermines confidence in the effectiveness of regulatory provisions.
2. In government services, citizens who identify errors in their NIN records often face long delays and repeated requests for documentation before any correction is made. For some, the process takes months, delaying access to critical services.
3. In banking, while requests for account information are generally honoured, the process often involves excessive study work, branch visits, and long waiting times. The right exists but is encumbered by inefficiencies that make it difficult to exercise smoothly.

These examples underscore that while rights exist legally, their realisation depends heavily on the institutional context, technical capacity, and willingness of organisations to respond.

5.5 Comparative Insight

A useful comparison can be drawn with the European Union under the GDPR. There, organisations are legally required to respond to data subject requests within a fixed timeframe, usually one month.[329] Failure to comply can result in strict penalties, including heavy fines that act as strong deterrents. The regulatory environment is backed by well-resourced data protection authorities that have the capacity to investigate complaints and enforce compliance.

By contrast, Nigeria's NDP Act provides for similar rights but lacks strong enforcement and practical mechanisms to ensure timely responses. Organisations are less afraid of penalties, and regulators are less capable of imposing them consistently. This difference highlights the importance

[329] GDPR, art 12(3)

of not just passing laws but building the institutions and cultures needed to make those laws effective.

5.6 Summary of the Gap

Overall, the policy practice gap in Nigeria reflects a combination of citizen unawareness, organisational unpreparedness, and weak enforcement. While the NDP Act sets out a robust legal framework, in reality, most Nigerians struggle to exercise their rights effectively. Awareness is low, compliance systems are underdeveloped, and enforcement actions are infrequent.

If left unaddressed, this gap risks undermining trust in Nigeria's digital transformation. Citizens may become sceptical about the promises of data protection, and organisations may continue to treat compliance as optional. Closing this gap is therefore not only about legal compliance but about ensuring that Nigeria's digital ecosystem is trustworthy, inclusive, and sustainable.

6. Barriers to Effective Implementation

6.1 Technical and Infrastructural Limitations

Many Nigerian organisations lack the technical systems needed to process data subject requests efficiently. Automated mechanisms, such as online portals for access or rectification requests, are rare. Instead, organisations often rely on manual processes, which lead to delays, errors, and poor record-keeping. Smaller businesses, in particular, face cost constraints in adopting compliance technologies, leaving them unable to meet the standards set by the NDP Act.[330]

6.2 Low Levels of Public Awareness and Digital Literacy

Even where legal rights exist, they are ineffective if citizens are not aware of them or do not understand how to exercise them. Public awareness of the NDP Act remains low, especially outside major urban centres. Many citizens are unaware that they have the right to request access to their personal information, request corrections, or opt out of unwanted data use.[331] Furthermore, digital literacy levels remain uneven. For a significant portion of the population, engaging with rights such as data portability requires technical understanding that they may not possess. This lack of knowledge and confidence leaves citizens vulnerable to exploitation and undermines the NDP Act's intent to empower individuals.

6.3 Resource Constraints for Organisations

On the organisational side, many companies, particularly small and medium-sized enterprises (SMEs), lack the financial and technical resources to implement strong data protection practices. While large banks and telecommunications providers are beginning to set up compliance programs, SMEs often see data protection as an expensive burden rather than a necessity. They

---

[330] Olugbile, O., "Assessment of Nigeria's Data Protection Regulatory Impact on SMEs," LinkedIn (August 29, 2025) https://www.linkedin.com/pulse/assessment-nigerias-data-protection-regulatory-impact-olugbile-yux2f/

[331] "SURVEY: 57% Undergraduates Ignorant of Nigeria's Data Privacy Law," Foundation for Investigative Journalism (FIJ) (December 23, 2025). https://fij.ng/article/survey-57-undergraduates-ignorant-of-nigerias-data-privacy-law/

may not be able to afford Data Protection Officers, invest in secure IT systems, or train staff adequately. This creates an uneven compliance landscape in which only the largest organisations meaningfully implement the law, while others either ignore it or comply superficially.

6.4 Cultural Perceptions of Privacy

In Nigeria, privacy is often undervalued compared to convenience or access to services.[332] Many individuals are more concerned about immediate benefits, such as getting faster internet or easier access to loans, than about long-term risks associated with data misuse. This cultural attitude makes it harder to build demand for data subject rights, as many people do not see the exercise of these rights as a priority.

6.5 Weak Enforcement Mechanisms

The Nigeria Data Protection Commission (NDPC) is still in its early stages of development and faces significant resource constraints. While the law empowers the NDPC to investigate and sanction non-compliance, in practice, enforcement has been limited. Without strong examples of penalties or corrective action, organisations may feel less pressure to comply fully with data subject rights provisions.

6.6 Capacity Gaps for Data Protection Officers (DPOs)

Capacity gaps among Data Protection Officers (DPOs) have historically been a significant barrier to the effective implementation of data subject rights in Nigeria. While the NDP Act mandates the appointment of DPOs, early implementation challenges revealed inconsistencies in skills, training, and professional competence across organisations. In response to this gap, the Nigeria Data Protection Commission (NDPC) has taken deliberate steps to professionalise the DPO role and strengthen institutional capacity.

Through the General Application and Implementation Directive (GAID), the NDPC has formally domesticated DPO certification in Nigeria. Articles 11 to 14 and Schedule 3 of the GAID establish a mandatory certification framework for DPOs, with the Institute of Information Management (IIM) licensed by the Commission to conduct DPO certification.[333] This development represents a critical shift from informal or ad hoc appointments toward a structured and competency-based approach to data protection leadership.

Certification alone, however, is not treated as a one-time requirement. Under the GAID framework, DPO certificates are subject to renewal through the accumulation of Continuous Professional Development (CPD) points. This requirement ensures that DPOs intentionally and continuously upskill in response to evolving legal, technological, and regulatory developments in

---

[332] UNCTAD, *Digital Economy Report 2021: Cross-border Data Flows and Development: For Whom the Data Flow* (United Nations 2021) 142.
[333] Nigeria Data Protection Commission, *General Application and Implementation Directive*, Articles 11–14 and Schedule 3 (2025).

data protection. By linking certification renewal to CPD, the NDPC promotes sustained professional growth rather than static compliance.

In addition, the Commission has introduced a verification mechanism through its official verification portal, where IIM-certified DPOs can be authenticated. This enhances transparency, builds trust in organisational compliance structures, and allows regulators, employers, and the public to confirm the legitimacy of DPO credentials.

Collectively, these measures address earlier capacity limitations by ensuring that DPOs possess the appropriate skills, maintain professional relevance, and operate within a regulated accountability framework. While challenges remain, the mandatory certification and CPD requirements mark a significant step toward strengthening organisational readiness and improving the practical enforcement of data subject rights in Nigeria.

6.7 Organisational Priorities and Resistance

Some organisations view compliance with data protection laws as a burden rather than a value-adding activity. This perception is especially common among SMEs, where business survival and profitability are prioritised over compliance investments. Even in larger organisations, the lack of a clear return on investment for compliance activities can lead to half-hearted efforts in implementing data subject rights.

6.8 Limited Public Awareness Campaigns

While the NDP Act was a major step forward, there has been limited public communication about its prvisions. Few citizens know how to file a data access or erasure request, and organisations rarely provide clear guidance on these processes. This lack of public education creates a vicious cycle: individuals do not exercise their rights, and organisations feel less compelled to prepare systems for handling them.

6.9 Summary of Barriers

In short, Nigeria's challenges in implementing data subject rights go beyond the legal framework. Weak infrastructure, cultural attitudes, limited enforcement, poorly trained DPOs, and organisational resistance all contribute to the gap between policy and practice. Unless these barriers are addressed, the NDP Act will struggle to deliver on its mandate of empowering citizens and building trust in the digital economy.[334]

7. Bridging the Gap

7.1 Strengthening Regulatory Enforcement

Regulatory enforcement plays a central role in bridging the gap between data protection policy and practice in Nigeria. Under the Nigeria Data Protection Act (NDP Act, 2023), the filing of

[334] World Bank Group, *Nigeria Digital Economy Diagnostic Report* (World Bank 2019) 34–38 hdl.handle.net accessed 18 December 2025.

Compliance Audit Returns (CARs) by data controllers and processors is mandatory and serves as a key mechanism for monitoring organisational compliance with data protection obligations.

According to the Nigeria Data Protection Commission's 2024 Annual Report, a total of **4,691** compliance audit returns had been filed as of the reporting period (NDPC, 2024, p. 29).[335] While this figure reflects growing regulatory engagement, it remains modest when viewed against the size of Nigeria's digital economy and the number of organisations processing personal data.

The NDPC has also demonstrated its enforcement mandate through publicly disclosed sanctions against organisations such as Meta, Multichoice, and Fidelity Bank. These actions reinforce regulatory credibility and signal that compliance obligations apply to both multinational corporations and large domestic entities. However, enforcement actions against smaller and locally operating organisations remain limited, which may weaken compliance incentives at the grassroots level.

To strengthen enforcement further, the NDPC should expand visible sanctions to include more local entities and continue publishing compliance audit and enforcement statistics. Consistent, transparent enforcement will enhance accountability and support the practical realisation of data subject rights across Nigeria's data protection ecosystem.

7.2 Increasing Awareness and Education

Many Nigerians remain unaware of their data rights or how to exercise them. Bridging the policy-practice divide requires targeted public education campaigns, including radio, television, and digital platforms in local languages. Collaboration with civil society organisations, schools, and professional associations can further amplify awareness. For businesses and government agencies, mandatory training programs for staff handling personal data should be implemented to reduce errors and negligence. The success of data subject rights depends not only on the laws but also on people's knowledge of them.

7.3 Embedding Data Protection into Organisational Culture

Organisations often treat data protection as a compliance requirement rather than as part of their operational culture. To close this gap, companies should integrate data protection principles into their internal policies, staff training, and customer engagement processes. For example, setting up clear, user-friendly mechanisms for handling access or deletion requests can improve compliance and build public trust. Senior management should also take responsibility by embedding accountability structures such as data protection officers (DPOs), internal audits, and reporting mechanisms.

7.4 Leveraging Technology and Innovation

Technology and innovation are essential for closing the gap between data protection policy and everyday practice, particularly in how data subjects exercise their rights and address grievances.

---

[335] Nigeria Data Protection Commission (NDPC), *2024 Annual Report*, p. 29; see also NDPC enforcement notices and compliance reports published on the NDPC official resources portal.

Article 40 of the GAID requires that data controllers implement a standardised grievance notice process that enables data subjects to understand how to raise concerns and seek redress effectively.[336] By adopting digital platforms with clear, accessible grievance modules, organisations can ensure that data subjects can submit complaints, track the status of their cases, and receive timely updates transparently. Likewise, the NDPC can harness automated compliance monitoring tools, centralised complaint portals, and real-time analytics to identify patterns of non-compliance and respond proactively. When both regulators and organisations integrate these digital solutions, the result is a more efficient, user-centric, and transparent system that supports data subjects in exercising their rights and resolving issues in accordance with established standards.

7.5 Encouraging Collaboration and Best Practice Sharing.

Effective data protection requires active cooperation among government agencies, industry groups, and international partners. In 2024, the NDPC formalised several Memoranda of Understanding (MoUs) with both local and international organisations to strengthen capacity building, compliance, and data governance in Nigeria's evolving data protection landscape.[337] One notable agreement was signed with the Small and Medium Enterprises Development Agency of Nigeria (SMEDAN), which aims to support roughly 40 million SMEs by providing training, awareness, and technical guidance on data privacy compliance under the Nigeria Data Protection Act. Through this partnership, NDPC and SMEDAN agreed to establish a working group dedicated to building data protection competencies and promoting best practices among micro, small, and medium enterprises. These collaborative arrangements enable organisations to exchange knowledge, align regulatory expectations, and adapt proven models, thereby accelerating practical adoption of data rights management and instilling a culture of compliance across sectors. By fostering such multi-stakeholder collaboration, the NDPC promotes a shared commitment to data protection excellence and encourages a "race to the top" where institutions strive for stronger compliance and heightened public trust.

8. Conclusion and Recommendations

8.1 Recommendations

To strengthen the protection of data subject rights in Nigeria, this study makes the following key recommendations:

- ***Enhance Regulatory Enforcement*** – The NDPC should adopt proactive audits, publish enforcement actions, and establish dedicated complaint-resolution units.
- ***Invest in Awareness and Education*** – Nationwide campaigns in multiple languages should inform citizens of their rights, while organisations should train staff to reduce non-compliance.

---

[336] Article 40, "Data Subject's Standard Notice to Address Grievance (SNAG)," in **General Application and Implementation Directive (GAID) 2025**, Nigeria Data Protection Commission (NDPC), p. 46.
[337] NDPC, **2024 Annual Report**, p. 13, Nigeria Data Protection Commission (NDPC).

- ***Promote Organisational Accountability*** – Companies should integrate data protection into their culture by appointing DPOs, embedding compliance in workflows, and offering user-friendly rights-request processes.
- ***Leverage Digital Tools*** – Both regulators and organisations should deploy technology to simplify rights requests, monitor compliance, and increase transparency.
- ***Foster Stakeholder Collaboration*** – The NDPC should build partnerships with civil society, industry bodies, and international regulators to encourage best practice sharing and peer learning.

By implementing these measures, Nigeria can strengthen the protection of data subject rights, reduce the gap between policy and practice, and foster greater trust in its digital ecosystem.

8.2 Conclusion

The recognition of data subject rights under the NDP Act represents a critical step toward protecting personal data in Nigeria. However, the gap between policy and practice has limited the effectiveness of these rights in everyday reality. Many organisations still view compliance as optional, while individuals often remain unaware of their rights or how to exercise them. Bridging this divide requires a multi-pronged approach that combines stronger enforcement, public awareness, organisational accountability, and innovative tools that simplify compliance.

The Efficacy of Privacy Self-Management in the Era of Artificial Intelligence

Chukwuemezie Charles Emejuo[338] Francis Aondongu Wayo[339]
Olumide Timothy Ajayi[340]

ABSTRACT

Privacy self-management vests control in an individual by granting him rights which he can exercise to control how information about him is collected and used. As the dominant model of privacy protection, this self-management model has been embraced globally in extant privacy and data protection laws such as the Nigeria Data Protection Act (NDP Act) and the famous European General Data Protection Regulation (GDPR). Building on the works of scholars, such as Solove and Hartzog who have vehemently opposed this model of privacy protection, this paper examines the efficacy of privacy self-management in the era of artificial intelligence (AI). Through a doctrinal research methodology, relevant privacy legislations and academic works, including books and journal articles have been reviewed. Findings show that privacy self-management has already proven inadequate in regulating privacy in the digital space. This is due to challenges associated with consent and lack of requisite privacy knowledge and resources by people to control how information about them is collected and used. With AI, the issues are being exacerbated while new ones are created. Due to the essentiality of data to AI and the inevitable integration of the technology in all spheres of life, the paper recommends a rethinking of privacy regulation to capture the nuances and complexities of this new technology. Consequently, it is recommended that privacy regulation in the AI age should shift towards a social structure model that views privacy not merely as a private good but a public one in order to create a robust regulatory framework.

Keywords: Privacy; Artificial Intelligence (AI); Privacy Self-Management; Data Protection; New Technology

[338] University of Illinois, Springfield
charles.emejuo@gmail.com
[339] Youth Centre, International Law Association (Nigeria) Committee on AI and New Technologies
wayofrancisaondongo@gmail.com
[340] University of the Cumberlands
aolumide26@gmail.com

1. Introduction

Writing on the revolutionary effects of artificial intelligence (AI), Professor Edward Lee notes that: "Artificial intelligence (AI) disrupts. It disrupts businesses, the work-force, the law, and society in numerous ways—much of which we do not fully comprehend."[341] If there is one area that this disruption has been glaring, it is about the implications for privacy. Prior to the emergence and surge of AI, digital technologies had already focalized privacy discussions in legal discourse across the world due to the overwhelming impacts of such technologies. With the impacts of AI cascading around just like that of a genie let out of the bottle, the privacy discourse is again in a disruptive stage that calls to question the efficacy of extant regulations to safeguard the rights of people. This situation is heightened by the data-driven nature of AI, implying a shift towards a world hungrier for data more than ever.[342] AI implications for privacy are enormous and worrying as is evident in the temporary ban on ChatGPT by the Italian Government in 2023 and another scrutiny for breaching the European General Data Protection Regulation (GDPR) of 2018.[343] Against this backdrop, this paper seeks to examine the sufficiency of privacy self-management adopted in privacy regulations like the Nigerian Data Protection Act (NDP Act), the GDPR, and the California's Consumer Privacy Act (CCPA) to protect people from AI risks. Considering that privacy self-management has already been criticised in extant literature,[344] this discussion will expose some of the limitations of the self-management framework in the AI space as this new technology amplifies the already existing privacy challenges while creating new ones.[345] It is hoped that understanding the shortfalls of privacy self-management will lead to adopting a better approach towards privacy regulation in this new era. For many jurisdictions still considering how to regulate AI, insights from this study will be useful in shaping their policy frameworks.

2. Overview of Privacy and Artificial Intelligence

2.1. Privacy

2.2. While popular, privacy is one of those many legal concepts that is devoid of a universally accepted definition. Therefore, literature on the meaning of the term tilts towards a descriptive than definitive approach because it is considered as "an inherently nebulous and problematic concept".[346] Two of the famously cited authors on the definition of privacy, Brandeis and Warren, refer to it as "the right to be left alone".[347] Similarly, it has been defined as "the right of the individual to be protected against intrusion into his personal life or affairs, or those of his family,

---

[341] Edward Lee, "Introduction: Symposium – AI Disrupting Law," *Chi.-Kent L. Rev*., 100, no 1 (2025): 3. https://scholarship.kentlaw.iit.edu/cgi/viewcontent.cgi?article=4479&context=cklawreview

[342] Jennifer King and Caroline Meinhardt, "Privacy in the AI Era: Policy Provocations for a Data-Centric World" *Stanford University Human-Centered*, February 22, 2024. https://hai.stanford.edu/policy/white-paper-rethinking-privacy-ai-era-policy-provocations-data-centric-world

[343] Claudio Novelli *et al*., "Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity," *Computer Law & Security Review: The International Journal of Technology Law and Practice* 55, no 1 (2024): 106066. https://www.sciencedirect.com/science/article/pii/S0267364924001328

[344] Sophie C. Boerman, Sanne Kruikemeier and Frederik J. Zuiderveen Borgesius, "Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data," *Communication Research 48*, no 7 (2021) 953- 977. https://journals.sagepub.com/doi/pdf/10.1177/0093650218800915

[345] Kelly D. Martin and Johanna Zimmermann, "Artificial intelligence and its implications for data privacy," *Current Opinion in Psychology*, (2024): 58. https://www.sciencedirect.com/science/article/abs/pii/S2352250X24000423

[346] Olumide Babalola, *Privacy and Data Protection Law in Nigeria* (Lagos: Noetico Repertum Inc. 2021): 9.

[347] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no 5 (1890): 193-220 https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

by direct physical means or by publication of information".[348] Over the years, the contours of privacy have expanded beyond the Brandeis-Warren conception to cover the exercise of control about what is known about the person outside their domestic sphere and the exercise of control about how one is known.[349] Instructively, Prosser's exposition on privacy torts by enumerating four aspects of privacy protection have greatly influenced the development of the law of privacy, especially in the United States (U.S).[350] These torts are public disclosure of private facts; intrusion upon seclusion; appropriation of name or likeness, and false light.[351]

In an attempt to define privacy by aggregating the views of different authors, Babalola postulates that privacy is "a fundamental right protection afforded a natural person from undesired or unauthorised interference with his/her personal affairs or relationships by whatever means irrespective of the purpose."[352] Worth noting, the absence of a one-size-fits-all definition has not whittled down the development of privacy law.[353] This is evident in the evolution of the concept in accordance with societal realities, and this development has added more nuances to the concept amidst varying legal regimes which have given rise to synonymous concepts like data privacy or information privacy. Used interchangeably with data protection, data privacy "guarantees control over personal information and prevents unauthorised access, use or misappropriation of such information".[354] According to Solove, this category is broader than the idea of privacy as espoused by Prosser.[355] Without delving further into the taxonomy of privacy, which is beyond this discussion, it is important to note that privacy is viewed broadly in this paper to cover data privacy or data protection.

2.3. Artificial Intelligence

While AI has become a buzzword recently, thanks to the emergence of generative AI and large language models (LLMs) like OpenAI's ChatGPT and Google's Gemini, history shows that it is not a new concept.[356] Notwithstanding, the current notion of AI can be linked to Stanford Professor, John McCarthy who coined the term during a proposal at the Darthmouth Conference in 1956.[357] Gleaning from McCarthy's description of the concept, AI connotes a field of computer science that focuses on creating intelligent machines or "AI systems."[358] Meanwhile, the idea of AI as intelligent machines remains contested as authors, Solove and Hartzog observe that "there

---

[348] Enyinnna S. Nwauche 'The Right to Privacy in Nigeria," *CALS Review of Nigerian Law and Practice* 1, no 1 (2007): 64, 65.

[349] Daniela Ježová, "Principle of Privacy by Design and Privacy by Default," *Regionlal Law Review*, (2020) 127- 139. https://rlr.iup.rs/wp-content/uploads/2020/12/10-Jezova.pdf.

[350] Mohamad Albakjaji and Manal Kasabi, "The right to privacy from legal and ethical perspectives," *Journal of Legal, Ethical and Regulatory Issues* 24, no 5 (2021): 1-10.

[351] William Prosser, "Privacy," *California Law Review* 48, no 3 (1960): 383-423. https://lawcat.berkeley.edu/record/1109651?ln=en&v=pdf

[352] Babalola, *Privacy and Data Protection Law in Nigeria*, 17.

[353] E.S Nwauche, "The Right to Privacy in Nigeria," *CALS Review of Nigerian Law and Practice* 1, 1 (2007): 63.

[354] Babalola, *Privacy and Data Protection Law in Nigeria*, 24.

[355] Daniel J. Solove, *Understanding Privacy* (Massachusetts: Harvard University Press, 2008).

[356] Vincent C. Müller, "Philosophy of AI: A Structured Overview," in *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*, ed. Nathalie Smuha (Cambridge University Press, 2025): 40.

[357] John McCarthy et al., "A proposal for the Dartmouth Summer Research Project on Artificial Intelligence," (1955). http://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html >

[358] Wannes Meert, Tinne De Laet, and Luc De Raedt, "Artificial Intelligence: A Perspective from the Field," in *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*, ed. Nathalie Smuha (Cambridge University Press, 2025): 17

is still nothing intelligent about Artificial Intelligence."[359] Instead, they view what is known today as AI as an "effective rebrand of algorithms and data in automated systems that can calculate inferences based on patterns in massive quantities of data".[360] Notwithstanding, the European Union Artificial Intelligence Act provides a broad definition of AI as follows:

AI system' means a machine-based system designed to operate with varying levels of autonomy, that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate output such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.[361]

The definition by the AI Act concerns itself with the product and not necessarily the science of AI. Thus, it can be extrapolated that while AI may be referred to as the field of computer science, AI systems are the products of that field. Herein, the term AI is used broadly to cover both the science and its results or products (systems) in so far as they affect privacy.

3. Privacy in the Age of Artificial Intelligence

On one hand, AI offers promising opportunities, while on the other hand, it presents new challenges that have altered how privacy is perceived and protected. Thus, significant literature on AI has focused on the implications of this technology on privacy.[362] In their study, Jobin, Ienca and Vayena named privacy amongst five other recurring themes in eighty-four published ethical principles on AI.[363] The others are "transparency, justice and fairness, non-maleficence, responsibility …"[364] Similarly, Fjeld and others identified privacy as one of the key emerging normative issues.[365] These findings are corroborated by sectoral analysis of AI in areas like health, education, trade, and health which all bring to the fore emerging privacy concerns.[366] This situation is driven by the fact that AI-related activities are data-driven – from the input to the outputs.[367] The quality of an AI system is dependent on the data it is trained with, hence, "it is no secret that data is the fuel of artificial intelligence systems …"[368] Furthermore, the deployment

---

[359] Daniel Solove and Woodrow Hartzog, "Kafka in the Age of AI and the Futility of Privacy as Control," *Boston University Law Review* 104, (2024): 1039.
[360] *Ibid*, 1021.
[361] EU Artificial Intelligence Act 2024, Article 3.

[362] Alfred Akakpo *et al*., "Artificial Intelligence (AI) and the Future of Information Privacy: Expert Viewpoints," *Journal of Global Information Management* 33, no 1(2025). https://www.igi-global.com/article/artificial-intelligence-ai-and-the-future-of-information-privacy/383050

[363] Anna Jobin, Marcello Ienca and Effy Vayena, "The Global Landscape of AI Ethics Guidelines," *Nature Machine Intelligence* 1, no 9 (2019):389–399.

[364] Inge Molenaar *et al*., "Artificial Intelligence and Education: Different Perceptions and Ethical Direction" in *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*, ed. Nathalie Smuha (Cambridge University Press, 2025): 271.
[365] Jessica Fjeld, J. *et al*., "Principled artificial intelligence: Mapping consensus in ethical and rights based approaches to principles for AI," *SSRN Electronic Journal*, (2020). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3518482
[366] Dayanand Naik, "Exploring the Pros and Cons of Artificial Intelligence (AI): Implications for Human Rights and Artificial Intelligence Development in India," *International Journal of Research Culture Society* 7, no 3 (2023) 100-104. https://ijrcs.org/wp-content/uploads/IJRCS202303021-min.pdf; Nathalie Smuha, ed. *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence* (Cambridge University Press, 2025).
[367] Daniel Solove, "Artificial Intelligence And Privacy," *Florida Law Review* 77, (2025): 1-73.

[368] Zanda Davida and Dominik Lubasz, "Privacy by Design – Searching for the Balance Between Privacy, Personal Data Protection and Development of Artificial Intelligence Systems," in *Internet and New Technologies Law* (2021) 337- 360, 337. https://www.researchgate.net/publication/357800084_Privacy_by_Design_-_Searching_for_the_Balance_Between_Privacy_Personal_Data_Protection_and_Development_of_Artificial_Intelligence_Systems

and use of AI leads to interactions with peoples' private lives, thereby, raising various privacy concerns.

To operate effectively, AI systems interact with a wide array of data: from personal information on a mobile device to browsing history and third-party systems like financial statements.[369] The various phases in the lifecycle of an AI contain many privacy risks. At the design and inception stage where decisions are made about what data to collect, there is the risk of collecting personal information, and during the data preparation and preprocessing stage which include cleaning the data for training, there are risks of breaching privacy rights during collection and including personal information. Other stages, including development, model training; verification and validation; deployment; operation and monitoring; re-evaluation, maintenance and updates, and retirement (when data associated with the model is archived or deleted) also contain various privacy risks.[370] And while humans can forget things, AI does not, hence issues like the enforcement of the right to be forgotten in the case of AI appears as a Sisyphean task. The black box nature and opacity of AI leave little to no room for transparency,[371] whereas privacy regulations demand transparency and accountability.[372] Additionally, privacy enforcement generally remains challenging with regards to AI due to lack of clarity on apportionment of rights and liabilities when a violation occurs. All these have added layers of complexity to how privacy is viewed and regulated. In a ruling in a case involving OpenAI, Inc. this year, a U.S Court ordered the AI giant to "preserve and segregate all output log data that would otherwise be deleted on a going forward basis until further order of the Court . . . , whether such data might be deleted at a user's request or because of 'numerous privacy laws and regulations' that might require OpenAI to do so."[373] From a privacy point of view, the ruling raises serious concern by interrupting with the right to erasure or data deletion, while resuscitating the adage that "everything on the Internet lives forever".[374] As these concerns are brought to the fore, whether existing privacy laws are sufficient to handle these issues is still debatable, and one way to find an answer is by examining the theoretical underpinning of current privacy regulation in the form of privacy self-management.

4. Privacy Self-Management

Regarded as the dominant and current model of privacy regulation,[375] privacy self-management refers to the system of regulation based on the grants of rights to individuals to control their privacy.[376] Through consent, individuals can decide what information to share. While the origins of privacy self-management can be traced to the Fair Information Practice Principles (FIPPs) which came into appearance in 1973 in a report by the U.S. Department of Health, Education,

---

[369] Isabel Barberá, "AI Privacy Risks & Mitigations – Large Language Models (LLMs)," *European Data Protection Board* (2025) https://www.edpb.europa.eu/system/files/2025-04/ai-privacy-risks-and-mitigations-in-llms.pdf

[370] *Ibid*.

[371] E Salami and I Nwankwo, "Regulating the privacy aspects of artificial intelligence systems in Nigeria: A primer," *African Journal on Privacy & Data Protection* 1, (2024): 220-247.

[372] See Nigerian Data Protection Act 2023 (NDP Act), section 24; GDPR, Articles 5&6.

[373] Justin Sorrell, "AI Privacy Implicated in Court Ruling," *Riley Bennett Egloff LLP*, July 1, 2025. https://rbelaw.com/ai-privacy-implicated-in-court-ruling/

[374] *Ibid*.

[375] Privacy Self-Management in a Click Happy Society, September 25, 2023. https://www.ramonzamora.co/p/privacy-self-management-in-a-click

[376] Daniel J. Solove, "Introduction: Privacy Self-Management and the Consent Dilemma," *Harvard Law Review* 126, (2013): 1880- 1903.

and Welfare (HEW) to address concerns around data digitization, it has influenced privacy regulation globally. It is currently embodied in many privacy and data protection laws globally, including the GDPR, which is the crown jewel of data protection regulation.[377]

Privacy self-management operates by granting individuals rights to self-manage their privacy.[378] According to Solove, "these rights consist primarily of rights to notice, access, and consent regarding the collection, use, and disclosure of personal data".[379] These rights can be gleaned from part six of the NDP Act which grants data subjects the rights to obtain from a data controller relevant information about them, right to data collection, data correction, and erasure;[380] the right to withdraw consent at any time concerning the processing of their personal information;[381] right to object to the processing of their personal information;[382] right not to be subject to a decision based solely on automated processing of personal data,[383] and right to personal data portability.[384]

The hallmark of privacy self-management is consent; thus, the lawful basis for processing personal data rests on the position that consent is given and not withdrawn.[385] This consent is required to be freely and intentionally given, and a request to obtain consent is to be in clear and simple language and accessible format.[386] Vested with the various rights which can be exercised through a consent model, "people are expected to make privacy decisions based on cost–benefit evaluations and to disclose data only when the benefits outweigh the costs"[387] and the individual is trusted to be well-informed enough to make rational and sensible decisions about their privacy. Characteristically, privacy self-management is modeled after individualism. Meanwhile, this individualistic notion of privacy fails to take cognizance of social structures and non-Western ideals, such as in Africa where individualism contradicts with the communitarian nature of the people and approach to things.[388] While privacy self-management has been successful to some extent, further appraisal in the following section will reveal the challenges associated with it generally and in the context of AI.

5. Assessing the Effectiveness of Privacy Self-management

Before considering whether privacy self-management is fit for purpose in the context of AI, it will be advisable to look at it generally because prior to the AI buzz, it had attracted both acceptability and criticisms. While noting the importance of privacy self-management, Solove criticises it for being inadequate in doing the task it is vested with.[389] He went on to identify fundamental defects

---

[377] Tuukka Lehtiniemi and Yki Kortesniemi, "Can the obstacles to privacy self-management be overcome? Exploring the consent intermediary approach," Big Data & Society (2017): 1. https://journals.sagepub.com/doi/10.1177/2053951717721935

[378] *Ibid.*

[379] Solove, "Introduction: Privacy Self-Management and the Consent Dilemma," 1880.

[380] NDP Act, section 34.

[381] *Ibid*, section 35.

[382] *Ibid*, section 36.

[383] *Ibid*, section 37.

[384] *Ibid*, section 38.

[385] NDP Act, section 25.

[386] Ibid, 26.

[387] Lehtiniemi and Kortesniemi, "Can the obstacles to privacy self-management be overcome? Exploring the consent intermediary approach," 2.

[388] Mubarak Raji, Devyn Wilder, Valentine Ugwoke and Masooda Bashir, 'An Assessment the enforcement mechanism in African data protection law," *African Journal on Privacy & Data Protection* 2, 1 (2025)

[389] Solove, "Introduction: Privacy Self-Management and the Consent Dilemma," 1880- 1903.

with privacy self-management that render it incapable of protecting people from privacy harms. These defects are cognitive and structural in nature. The cognitive challenge of privacy self-management emanates from the supposition that people are generally rational and informed to make right decisions about their privacy, whereas studies show that the ability of people to make decisions does not fit into this vision of privacy self-management.[390] The idea that people are informed about privacy is fallacious because in practice, they lack the requisite knowledge and resources to make well-informed decisions.[391] Even when presented with the information in form of privacy notices and policies, the decisions of the people are skewed by factors beyond their control. Assuming people are informed enough, Solove argues that structural problems emerge in form of the scale of activities needed to manage their privacy considering the multiplicity of parties involved in data collection, processing and use.[392] The scale of information people may need to read and the various channels they will have to navigate make it too daunting a task to undertake. A research shows that an average American visits not less than 1,354 sites a year, and reading all their privacy policies in full will take at least 76 working days.[393] An earlier study estimated that a person will need 80–300 hours to get acquainted with privacy policies of websites s/he visits in a year.[394] Another structural problem arises from the fact that individuals may not be able to predict how small pieces of information about them may be aggregated in the future to reveal more than what they had intended to share. These problems are further compounded by the challenge of assessing the cost and benefits of deciding to share their data. While people may be influenced by short-term benefits, the long-term detriments are often overlooked as they may appear innocuous at the time of making the decision.[395]

Privacy self-management rests on consent but the foregoing exposition reveals that the type of consent people are engaged in is murky due to various reasons. Privacy policies are complicated and many people do not read privacy policies before consenting.[396] A survey of 2,000 people in the U.S revealed that 91% consent to legal terms and service conditions without reading.[397] Even when people read, these policies are too complicated and sometimes incomprehensible even for privacy professionals.[398] Struggling with understanding them lead to resignation by giving up privacy.[399] Thus, the current consent model has been criticised for being "… operationalised in problematic

---

[390] *Ibid.*

[391] Yaqoub Alsarkal, Nan Zhang and Heng Xu, "Protecting Privacy on Social Media: Is Consumer Privacy Self-Management Sufficient?" *Proceedings of the 52nd Hawaii International Conference on System Sciences*, (2019): 4875. https://scholarspace.manoa.hawaii.edu/bitstreams/2d7ff2a1-0671-4786-8b0f-4a6f2f805be0/download

[392] Solove, "Introduction: Privacy Self-Management and the Consent Dilemma," 1880-1903.

[393] Lorrie Faith Cranor and Aleecia McDonald, "Digital Life in 2025: The Future of Privacy," *Pew Research Center* 28, (2014). http://www.pewinternet.org/files/2014/12/PI_FutureofPrivacy_1218141.pdf;
Privacy Self-Management in a Click Happy Society, September 25, 2023. https://www.ramonzamora.co/p/privacy-self-management-in-a-click

[394] Aleecia M McDonald and Lorrie Faith Cranor, "The cost of reading privacy policies," *I/S: A Journal of Law and Policy for the Information Society* 4, no 543 (2008): 1–22. https://kb.osu.edu/server/api/core/bitstreams/a9510be5-b51e-526d-aea3-8e9636bc00cd/content

[395]Solove, "Introduction: Privacy Self-Management and the Consent Dilemma," 1880- 1903.

[396] Solove and Hartzog, "Kafka in the Age of AI and the Futility of Privacy as Control."

[397] David Medine and Gayatri Murthy, "Making Data Work for the Poor: New Approaches to Data Protection and Privacy," *Consultative Group to Assist the Poor*, (2020).

[398] Gitanjali Das and others, "Privacy Policies for Apps Targeted Toward Youth: Descriptive Analysis of Readability," *JMIR Mhealth Uhealth* 6, no 1 (2018). https://mhealth.jmir.org/2018/1/e3/.

[399] Annmarie Hanlon and Karen Jones, "Ethical concerns about social media privacy policies: do users have the ability to comprehend their consent actions?," *Journal of Strategic Marketing*, (2023). https://www.tandfonline.com/doi/abs/10.1080/0965254X.2023.2232817.

ways, for all users",[400] thereby, leading itself to what Solove refers to as fictitious consent,[401] or "unwitting consent, coerced consent, and incapacitated consent".[402] Peoples' consent is undermined[403] by information and power asymmetries between the individuals and platforms dealing with their data.[404]

Furthermore, the operationalisation of privacy self-management promotes the theory of the privacy paradox which supports less privacy protection. The privacy paradox connotes the discord between peoples' stated claims about privacy versus their actions or behaviours.[405] Based on this theory, people claim to value privacy yet easily relinquish their privacy or take less steps than minimally required to protect their personal information.[406] This leads to the conclusion that people do not actually value privacy, hence protection should be relaxed. However, research shows that their behaviours do not reflect the true value of privacy as those behaviours are context-specific and there are several factors that play a part in undermining the appropriateness of their decisions.[407] Arguing that the individual is doomed to fail, hence he should not be blamed for behaving in a manner contradictory to his avowed claim to value privacy, Obar termed this system as the fallacy of data privacy self-management where "… you have largely been placed in an impossible scenario …. whereby governments and industry allow the game to continue without ensuring the rules are fair for all the players".[408] Also termed the "unattainable ideal", this self-management idea assumes that a person could sufficiently deal with all the complexities concerning her/his privacy.[409] However, even when people take necessary steps, such as "limiting their profile visibility and constraining their friending behaviors, it does not necessarily mean they will reduce self-disclosure on SNSs [social networking sites] because these behaviours are predicted by different factors".[410] Thus, the individual is handicapped and doomed to fail in attempting to protect her/his privacy.

Privacy self-management also leads to a limited conception of privacy through the lens of individualism by making privacy protection about "I" or "me" and not "we". This occludes a social understanding of privacy and obstructs a better framing of the concept within the society.[411]

---

[400] Reset. Tech Australia, "Can the consent model improve the digital world, especially for young people?," *Policy Briefing* (2023): 7 https://apo.org.au/node/322895 .

[401] Daniel J. Solove, "Murky Consent: An Approach to the Fictions of Consent in Privacy Law," *Boston Law Review* 104, (2024): 593. https://www.bu.edu/bulawreview/files/2024/04/SOLOVE.pdf.

[402] Neil Richards and Woodrow Hartzog, "The Pathologies of Digital Consent," *Wash. U. L. Rev. 96*, (2019): 1461, 1478. https://openscholarship.wustl.edu/law_lawreview/vol96/iss6/11

[403] Mario Pascalev, "Privacy exchanges: restoring consent in privacy self-management," *Ethics and Information Technology* 19, (2017): 39–48.

[404] Alessandro Acquisti, Curtis Taylor and Liad Wagman, "The Economics of Privacy," *Journal of Economic Literature* 54, no 2 (2016): 442. https://www.aeaweb.org/articles?id=10.1257/jel.54.2.442

[405] Daniel Solove, "The Myth of the Privacy Paradox," *The George Washington Law Review* 89, no 1 (2021) 1, 1. https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2738&context=faculty_publications.

[406] Ibid.

[407] Perla Khattar, "What You Don't Know Will Hurt You: Fighting the Privacy Paradox by Designing for Privacy and Enforcing Protective Technology," Wash. J. L. Tech. & Arts 18, (2023): 1 https://digitalcommons.law.uw.edu/wjlta/vol18/iss4/1/.

[408] Jonathan A. Obar, "Searching for Data Privacy Self-Management: Individual Data Control and Canada's Digital Strategy," *Canadian Journal of Communication Policy Portal* 44, no 2 (2019): 35.

[409] *Ibid.*

[410] Hsuan-Ting Chen and Wenhong Chen, "Couldn't or Wouldn't? The Influence of Privacy Concerns and Self-Efficacy in Privacy Management on Privacy Protection," *Cyberpsychology, Behavior, and Social Networking* 18, no 1 (2015): 13.

[411] Gordon Hull, "Successful failure: what Foucault can teach us about privacy self-management in a world of Facebook and big data," *Ethics and Information Technology* 17 (2015): 89–101.

Instead, privacy is individualised and commodified as something worth trading than protecting.[412] The sharing of personal information inadvertently leads to disclosing information about others. These spillovers, which form privacy externalities[413] are often overlooked due to the focus on privacy as a private good instead of a social good or public good.[414] Since the conduct of one's activities affects others, the protection of one's privacy cannot be done in isolation of "others",[415] hence Professor Cohen is reported to have argued that "[P]rivacy incursions harm individuals, but not only individuals. Privacy incursions in the name of progress, innovation, and ordered liberty jeopardise the continuing vitality of the political and intellectual culture that we say we value."[416]

Having exposed the defects of privacy self-management, it suffices to note that since it has been expressed that AI, in addition to creating new privacy challenges, amplifies and complicates the existing ones, the effectiveness of privacy self-management is further challenged. Therefore, the problems of murky consent, complicated privacy policies, lack of requisite privacy knowledge and resources to enforce one's privacy rights are exacerbated by AI. Privacy self-management operates on the belief that users of technologies are informed but it is already established that this is not true. With AI, no one is knowledgeable about what transpires in the system due to the black box nature and opacity of the technology.[417] Due to the low level of AI literacy, users of the technology are more prone to confusion, hence their consent given in relation to an AI activity cannot be considered to be freely given. In some cases, consent may not be obtained at all. In a recently decided case in South Korea, the judge found that in training its chatbot, Lee Luda, data of about 600, 000 users, including their chat history, was used by Scatter Lab without obtaining permission.[418] The court held that there was no consent as Scatter Lab failed to clearly inform its users about the collection of their personal chats to train its AI. Consequently, damages were awarded against Scatter Lab for privacy violation. This case illustrates the challenge with consent in the context of AI.

The issue of data aggregation is also further problematised by AI which makes it possible for systems to infer information not originally shared by an individual.[419] Similarly, the acceleration and proliferation of deepfakes by AI raise significant privacy concerns that relying on privacy self-management will not provide adequate answers.[420] AI privacy risks do not only apply to individuals but societies at large, challenging the individualistic conception of privacy under the self-management framework. Highlighting the privacy risks posed by AI, Jennifer King and Caroline Meinhardt note that the current privacy laws modeled after the Fair Information Practice

---

[412] *Ibid.*

[413] Simeon de Brouwer, "Privacy self-management and the issue of privacy externalities: Of thwarted expectations, and harmful exploitation" *Internet Policy Review* 4, (2020): 1-29, https://doi.org/10.14763/2020.4.1537

[414] Debbie V.S. Kasper, "Privacy as a Social Good," *Social Thought & Research* 28 (2007): 165.

[415] Joshua A.T. Fairfield and Christoph Engel, "Privacy As a Public Good," *Duke Law Journal* 65, no 3 (2015): 385.

[416] Solove and Hartzog, "Kafka in the Age of AI and the Futility of Privacy as Control," 1029.

[417] Blake Murdoch, "Privacy and artificial intelligence: challenges for protecting health information in a new era," *BMC Med Ethics* 22, (2022): 122.

[418] Kim Nam-Young, "Chatbot Lee Luda popular for sounding natural, until users realized it used data from private chats," *Korea JoongAng Daily*, July 7, 2025. https://koreajoongangdaily.joins.com/news/2025-07-17/national/socialAffairs/AI-chatbot-Lee-Luda-popular-for-sounding-natural-until-users-realized-it-used-data-from-private-chats/2353227.

[419] Immaculeta Chidera Onyekwe, "AI and Data Privacy in the Internet of Things (IoT): A New Frontier in the Connected World," *NDPC –International Journal of Data Privacy and Protection* 1, (2024): 26.

[420] Motunrayo Adebayo, "Deepfakes and Data Privacy: Navigating The Risks in the Age of AI," *NDPC –International Journal of Data Privacy and Protection* 1, (2024): 107.

Principles (FIPPs) from which privacy self-management sprang out, implicitly address some of the privacy issues but fall short of being adequate.[421] This is largely because FIPPs were not designed with the anticipation of AI systems like generative AI and LLMs.[422] Therefore, the failure of privacy self-management to offer adequate privacy protection cannot be diffused from its theoretical basis. The fact that this privacy-control paradigm has fallen short in capturing the broader privacy concerns in the 21st century calls into question the application of privacy self-management in the context of AI when this new technology renders people more powerless, buttressing the position of people having control over their data as illusory. [423]

6. Charting a Way Forward Away from Privacy Self-Management

Having exposed the problem with privacy self-management, the discussion will be better wrapped up by suggesting a way forward. Should privacy self-management be reimagined to apply differently to AI? Or should an alternative be explored? It is clearly established that the problem with the privacy self-management model is a fundamental one that has lingered on for years. Towards the exodus of the 20th century and the genesis of the 21st century, scholars brought to attention the limitations of privacy in the internet era and these concerns have not been fully addressed till date.[424]

To give meaning to privacy, as a concept whose contours keep expanding, the suggestion herein is to move away from privacy self-management and more closely to the societal structure model advocated by scholars like Solove who have emerged as prominent critics of the self-management model.[425] The social structure model views privacy not merely as a private good but a social and public one. It underlines the inconsequentiality of the individual in the grand scheme of things, thereby broadening the conception of privacy to capture its true value in society and to take structural reforms of the systems that have hitherto undermined effective privacy protection. To this school of thought, as noted by Solove and Hartzog, "privacy is first and foremost about power and how human information is relevant in its creation, deployment, and distribution".[426] This could not be truer than in the AI age where global powers are fighting over who wins a race that is mainly driven by information and data.[427] Interestingly, the EU AI Act embraces this approach

---

[421] King and Meinhardt, "Privacy in the AI Era: Policy Provocations for a Data-Centric World" *Stanford University Human-Centered.*

[422] Ibid.

[423] Paul M. Schwartz, "Internet Privacy and the State," *CONN. L. REv.*32, (2000): 815. https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://paulschwartz.net/wp-content/uploads/2019/01/SCHWARTZ-CK1A-1.pdf&ved=2ahUKEwj454rCxryPAxX-V0EAHa4sES0QFnoECDoQAQ&usg=AOvVaw1uuPEiXr11JR7852_dGq8Y

[424] Daniel J. Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy," *Stan. L. Rev.* 53, (2001) 1393; Anita Allen, "Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm," *Connecticut Law Review* 32 (2000): 861 https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://scholarship.law.upenn.edu/cgi/viewcontent.cgi%3Farticle%3D1789%26context%3Dfaculty_scholarship&ved=2ahUKEwi8-vTpxryPAxXOQEEAHQoRLYkQFnoECCQQAQ&usg=AOvVaw1ouqgidF26v1kzIfyf3KfY.

[425] Solove and Hartzog, "Kafka in the Age of AI and the Futility of Privacy as Control."

[426] *Ibid*, 1027

[427] *Ibid.*

like the Digital Services Act[428] by providing "substantive rules and duties aimed at limiting risk and harm regardless of an individual's consent or control".[429]

Another recommendation is to approach privacy regulation from a contextual perspective, following Nissenbaum's exposition on "privacy as contextual integrity.[430] Conceptual integrity as a privacy construct entails that to adequately protect privacy, the norms of particular contexts should be taken into consideration. Contextual integrity makes it imperative to understand the people involved in information gathering, analysis, and dissemination, the nature of the information, and the overall relationship of parties dealing with the information.[431] Contextual integrity underscores the significance of governing information flow to prevent leakages that may arise from mishandling the information.[432] This model does not contradict with the social structure model espoused by Solove. As noted by Kroger, Otto Hans-Martin Lutz and Stefan Ullrich, many of the regulatory possibilities that can be explored are far from exhausted.[433] Since the contextual integrity theory appears to be amenable to dominant norms, it can be instrumental in anchoring privacy regulation on a social structure model whereby the true value of privacy is accessed not on individualistic basis but societal norms. Consequently, it is argued that an effective privacy regulation in the AI age will require shifting the focus to those responsible for or involved in information gathering, processing and distribution.

7. Conclusion

AI is here to stay and there is no possibility to return the genie back to the bottle. Thus, humanity must take strategic steps to ensure that it does not live to regret giving away privacy too cheaply to machines or their owners. Privacy rights, as currently anchored on self-management have limitations and cannot sufficiently protect people against the risks posed by AI. Coupled with the individualistic conception of privacy, which is limiting, the unique features of AI have exacerbated privacy concerns while posing new ones which cannot be successfully addressed through an individual-based model. Consequently, there is need to adopt a different regulatory approach, hence the recommendation for further study and examination of the social structure model as well as the contextual integrity theory. This recommendation is not in dismissal of the contributions of privacy self-management in general but considering its many limitations, finding a better approach is advisable especially in this momentous age where everything needs to be done with caution, bearing in mind that how we approach AI today will shape the lives of future generations.

---

[428] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC, 2022 O.J. (L 277) 1.

[429] Solove and Hartzog, "Kafka in the Age of AI and the Futility of Privacy as Control," 1031.

[430] Helen Nissenbaum, 'Privacy as Contextual Integrity," Wash. L. Rev. 79, 119 (2004).

[431] *Ibid.*

[432] Adam Barth, Anupam Datta, John C. Mitchell and Helen Nissenbaum, "Privacy and Contextual Integrity: Framework and Applications" (2006) https://dl.acm.org/doi/10.1109/SP.2006.32

[433] Jacob Leon Kroger, Otto Hans-Martin Lutz and Stefan Ullrich, "The myth of individual control: Mapping the limitations of privacy self-management," (2021) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3881776

Building a culture of Data Protection: A Pedagogical Basis for Data Privacy Literacy in Nigerian Universities

Obimuyiwa Gabriel Ayodeji[434], Salekhova Leila Leonardovna[435], Owolabi Blessing Adejoke[436]

ABSTRACT

The implementation of the Nigeria Data Protection Act (NDP Act) 2023 imposes a substantial compliance obligation on Nigerian universities, which are becoming more data-intensive owing to rapid digitisation. A significant disparity arises between the technical-legal execution of the legislation and the development of a viable, ethical data protection culture inside these intricate organisations. This report contends that closing this gap is primarily an educational problem. It argues that transcending mere checkbox compliance calls for an integrated teaching effort to integrate data privacy awareness across the whole academic environment. The research utilises a qualitative, conceptual analysis to integrate ideas from data protection legislation, educational theory, and the particular setting of higher education in Nigeria. In addressing the recognised deficiency, the research introduces the Obimuyiwa, Salekhova & Owolabi - ETAP (Embedded, Tiered, and Applied Privacy Literacy) Framework. This concept promotes a multi-stakeholder approach, providing customised educational interventions to students, academic personnel, and administrative staff, designating them as empowered data subjects, the ethical data processors, as well as compliant operational agents, respectively. The framework prioritises incorporation into current curriculum and professional development, as well as real-world applications like as simulations along with projects, to guarantee relevance and sustainability. The discourse critically examines the ramifications of this pedagogical transition for institutional governance as well as strategic alignment with the NDP Act, while also addressing practical problems such as finance and opposition to change. The study argues that investing in this pedagogical framework is not just a statutory need but also a strategic priority for Nigerian universities to enhance resilience, promote digital citizenship, and effectively protect the rights of their academic populations in the digital era.

Keywords: Privacy, Educational, Frameworks, Universities, Data-Intensive

[434] *Institute of Bilingual and Digital Education,obimuyiwagabriel@gmail.com*
[435] *Kazan Federal University, Russia salekhova2009@gmail.com*
[436] *Nigeria Data Protection Commission bowolabi@ndpc.gov.ng*

1. Introduction

The rapid digitisation of higher education institutions worldwide has caused a fundamental change in the administration of academic and administrative data. This transformation in Nigeria is marked by the use of Learning Management Systems (LMS), biometric enrolment tracking, digital student information systems, and web-based research repositories[437]. Although new technologies provide operational efficiency and improved learning experiences, they simultaneously increase the volume and severity of personal data processing, resulting in unparalleled privacy hazards for students, professors, and staff[438]. The NDP Act 2023 addresses these challenges by instituting a vital regulatory framework that mandates organisations, including universities, to comply with principles of lawful gathering, accountability, and safeguarding the rights of data subjects[439].

However, a large gulf typically exists between the regulatory imposition of data protection and its true, internalised acceptance inside complex organisational cultures including those of universities[440]. Regulatory compliance is often seen as a technical or legal checklist (a set of rules to be formulated and audits to be successfully completed) instead of a fundamental ethical guideline that informs daily conduct[441]. This techno-legalistic methodology is intrinsically precarious. This may result in a situation where universities adhere to procedures but remain culturally susceptible, as the human components of the system (management, lecturers, along with students) may lack the essential literacy to make informed privacy choices in their daily operations[442]. The result is a compliance framework founded on unstable ground, susceptible to violations arising from ignorance rather than intent.

This gap highlights a crucial, albeit seldom examined, connection: the convergence of data security and education. The inquiry extends beyond the presence of a Data Protection Officer or a policy on privacy at a university; it concerns how a learning organisation acquires, implements, and eventually internalises the principles of data privacy. The prevailing debate, both in Nigeria and internationally, has mostly focused on the legal and technical aspects of data governance, while significantly overlooking the educational and behavioural strategies necessary for its maintenance[2]. Pedagogical theory posits that enduring transformation in institutional practice needs beyond an authoritative mandate; it demands the cultivation of literacy, the promotion of critical participation, and the incorporation of new norms into the essence of organisational identity[443].

---

[437] *Aleru, Gladys Ejimole. "Integration of digitalisation of personnel management in universities in Rivers State, Nigeria implications on lecturers' productivity." Journal of Association of Educational Management and Policy Practitioners 6, no. 1 (2024): 107-117.*

[438] Ebenibo, Lionel, Joy Onma Enyejo, George Addo, and Toyosi Motilola Olola. "Evaluating the Sufficiency of the data protection act 2023 in the age of Artificial Intelligence (AI): A comparative case study of Nigeria and the USA." *International Journal of Scholarly Research and Reviews* 5, no. 01 (2024): 088-107.

[439] Juma, Isaac, and Bukola Faturoti. "Enforcing data privacy in Kenya and Nigeria: towards an African approach to regulatory practice." *International Review of Law, Computers & Technology* (2025): 1-26.

[440] Borgman, Christine L. "Open data, grey data, and stewardship: Universities at the privacy frontier." *Berkeley Technology Law Journal* 33, no. 2 (2018): 365-412.

[441] Beach, Thomas H., Jean-Laurent Hippolyte, and Yacine Rezgui. "Towards the adoption of automated regulatory compliance checking in the built environment." *Automation in construction* 118 (2020): 103285.

[442] Akintola, Simisola O., and Dorcas A. Akinpelu. "The Nigerian Data Protection Regulation 2019 and data protection in biobank research." *International Data Privacy Law* 11, no. 3 (2021): 307-318.

[443] Daramola, Dorcas Sola, and Gabriel Ayodeji Obimuyiwa. "Effects Of Manual And Computer-Based Concept Mapping Innovative Strategies On Academic Performance Of Pre-Service Teachers In Kwara State Colleges Of Education." *Epiphany* 15, no. 2 (2023): 118-139.

This difficulty is especially pronounced in the Nigerian setting. Higher Education Institutions sometimes contend with outdated infrastructure, constrained financial resources, and an urgent need to align with global digital advancements, often compromising simultaneous investment in digital citizenship and ethics[444]. The outcome is a setting where sophisticated technologies are implemented in an environment perhaps ill-equipped for the associated data obligations, resulting in a precarious situation of risk and non-compliance. This study contends that attaining substantial compliance with the NDP Act at Nigerian colleges depends on the intentional establishment of a data protection culture, thereby presenting a pedagogical challenge. The research advances beyond just recognising the issue to proposing a complete, multi-stakeholder educational framework for integrating data privacy literacy all over the university environment. This research seeks to provide a pragmatic path by using recognised theories of institutional transformation and adult learning, specifically tailored to the Nigerian higher education system. This study aims to address the primary research question: What defines an effective educational framework for promoting data privacy literacy and establishing a sustainable culture of data protection in Nigerian universities?

This research enhances the academic discussion on sectoral trends in data privacy, specifically in education within the Global South, and provides practical advice for policymakers at the Nigeria Data Protection Commission (NDPC), higher education officials, and academic staff developers responsible for implementing legal mandates in institutional practices.

2. Literature Review

The establishment of data protection in Nigeria signifies a substantial transition from ambiguous principles to a framework of defined legal responsibility. Before the NDP Act 2023, the regulatory framework was characterised by a fragmented array of provisions, particularly Section 37 of the 1999 Constitution, which ensures the right to privacy[445], and the National Information Technology Development Agency (NITDA) Data Protection Regulation of 2019[6,446]. Academics have mostly examined this first phase as one characterised by emerging awareness and inadequate enforcement, whereby compliance was often seen as a mere formality rather than an essential operational norm.

The implementation of the NDP Act 2023, which created the Nigeria Data Protection Commission (NDPC), signifies a significant legal advancement. Current legal assessments have begun examining its rules, making similarities with established frameworks such as the EU's General Data Protection Regulation (GDPR)[447]. The preliminary analyses concentrate on the Act's essential provisions, legal grounds for processing, rights of data subjects, responsibilities of Data Protection Officers, and the consequences for international data transfers[3]. Solove[448]

---

[444]Obimuyiwa, G. A., & Salekhova, L. L. "Stages of the formation of higher education in Nigeria in the 20th century: from colonial colleges to national universities". *Pedagogy. Questions of Theory and Practice* 10, no. 8 (2025): 1198-1205.

[445] Kusamotu, Ayo. "Privacy law and technology in Nigeria: The legal framework will not meet the test of adequacy as mandated by article 25 of European union directive 95/46." *Information & Communications Technology Law* 16, no. 2 (2007): 149-159.

[446] Babalola, Olumide. "The EU GDPR and Nigeria's NDPR: A comparative analysis." *Journal of Data Protection & Privacy* 4, no. 4 (2021): 372-387.

[447] Aloamaka, PC Aloamaka. "Data protection and privacy challenges in Nigeria: Lessons from other jurisdictions." *UCC Law Journal* 3, no. 1 (2023): 281-321

[448] Solove, D.J., 2021. The myth of the privacy paradox. *Geo. Wash. L. Rev.*, *89*, p.1.

contends that a solely statutory analysis may engender a compliance paradox, whereby organisations prioritise evading legal penalties above cultivating genuine respect for privacy. The existing literature on the NDP Act, while crucial, mostly resides within the legal and regulatory sphere, with little focus on the mechanisms for implementation in intricate, human-centered sectors such as education.

A rising number of researchers globally are critiquing the constraints of a techno-legalistic framework for data governance. Ullagaddi[449] persuasively contends that robust data protection calls for a cultural transformation inside organisations, beyond mere checklists to include privacy as a collective value. This corresponds with fundamental organisational theory, particularly Fullan's (2016) research on educational transformation, which asserts that enduring innovation relies on changing the beliefs, attitudes, and norms of people inside the organisation.

The notion of data privacy literacy serves as an essential link between legal frameworks and cultural practices. It transcends fundamental awareness to include the information, skills, and attitudes necessary for people to effectively manage their personal data and comprehend their rights and duties[11]. Within a university environment, this constitutes not a single talent but a continuum of skills. For a student, it may include comprehending the use of their data by a learning analytics system. For a researcher, it involves formulating studies that include privacy-by-design principles. For an administrator, it entails understanding the processes for managing a data breach. Although models for digital literacy, which include Sharikov's four-component model[450], and structures for general data literacy are available, the literature indicates a notable absence of frameworks that specifically adapt these concepts to the functional and ethical conditions of a university setting, especially in a resource-limited context.

The Nigerian higher education industry is a distinctive and essential case study. Extensive research has shown the continuous digital transformation, driven by the demands for effectiveness, scale, and international competitiveness[451]. This has resulted in the extensive and often rapid adoption of technology like as Learning Management Systems (such as Moodle), biometric registration platforms, as well as digital academic records[452].

Nevertheless, researchers like Babalola[10] observe that this digitisation often transpires without corresponding investment in the soft foundations of policy, ethics, and human ability. Aloamaka[11] identifies significant obstacles, such as insufficient financing for cybersecurity, a deficiency in specialised staff training, and outdated paper-based methods that result in uneven data governance. This generates an optimal scenario in which sophisticated data-processing technologies are used in a setting inadequately prepared to address the related privacy problems. The particular vulnerabilities of students as data subjects, often contending with power disparities and bureaucratic intricacies, remain inadequately examined within the Nigerian setting,

---

[449] Ullagaddi, Pravin. "GDPR: Reshaping the landscape of digital transformation and business strategy." *International journal of business marketing and management* 9, no. 2 (2024): 29-35.
[450] Sharikov, Alexander. "Digital Literacy: a four-component model." *Zhurnal Issledovanii Sotsialnoi Politiki= The Journal of Social Policy Studies* 14, no. 1 (2016): 87.
[451] Mohamed Hashim, Mohamed Ashmel, Issam Tlemsani, and Robin Matthews. "Higher education strategy in digital transformation." *Education and information technologies* 27, no. 3 (2022): 3171-3195.
[452] Odoh, J. N., & Nwokwu, B. N. (2024). Analyses on the causes of ASUU strike and its perceived impact on the academic performance of the student of Nnamdi Azikiwe University, Awka. *African Journal of Educational Management, Teaching and Entrepreneurship Studies, 13*(1), 308-323.

highlighting a substantial deficiency in the sectoral study of the NDP Act's influence. This study aims to address this gap by enquiring not into the legal obligations, but rather into how a Nigerian institution might pedagogically cultivate the culture and literacy essential for sustainably and morally fulfilling that obligation. This section will delineate the technique for constructing the framework.

3. Methodology

The study utilises a qualitative research methodology and a multi-phased conceptual analytic technique to provide an instructional framework for data privacy literacy. The main aim is not to provide new empirical data, but to integrate existing information, ascertain best practices, and contextualise them within the distinct ecology of Nigerian institutions. The technique is organised into three separate stages, based on recognised procedures in the building of educational frameworks[453]. The current research focusses on the development of a conceptual framework. Jabareen[17] states that this process entails constructing a framework via the conceptual examination and review of existing literature, ideas, theories, and empirical facts. This methodology is especially appropriate for the research issue, as it facilitates the amalgamation of many fields (data protection legislation, pedagogical theory, as well as higher education studies) into a cohesive, implementable framework. The design progresses from a general comprehension to a particular, contextualised result, guaranteeing that the framework is both theoretically robust and practically relevant.

The data required for this conceptual investigation include existing textual sources that were methodically located and examined. The sources include Primary legislative and Policy Documents, with the NDP Act (2023) as the foundational legislative language, delineating the mandatory compliance criteria. Supplementary documents, including the NDPC's implementation instructions and specific university data protection policies, were examined to assess the present status of policy-practice alignment. A thorough study of academic literature was performed in three primary domains: data privacy and compliance, criticisms of techno-legalistic methodologies, and research on organisational culture. The pedagogical and andragogical theory utilises concepts from institutional transformation[454] , communities of practice[455], as well as adult learning principles[456] to guide learning practices. The study examined research on digital transformation, organisational obstacles, and sector-specific capabilities within the context of Nigerian higher education.

4. Proposed Framework for Data Literacy in Nigerian Universities

The study indicates that a universal training module is inadequate for fostering a strong culture of data security. This study offers a multi-stakeholder, tiered framework named the *Obimuyiwa, Salekhova & Owolabi – ETAP* (Embedded, Tiered, and Applied Privacy Literacy) Framework. The ETAP Framework is intended to be embedded inside educational institutions and academic life, transitioning from isolated seminars to ongoing, context-specific education. The framework is

---

[453] Jabareen, Yosef. "Building a conceptual framework: philosophy, definitions, and procedure." *International journal of qualitative methods* 8, no. 4 (2009): 49-62.
[454] Fullan, Michael. *Leading in a culture of change*. John Wiley & Sons, 2007.
[455] Wenger, Etienne. "Communities of practice: Learning as a social system." *Systems thinker* 9, no. 5 (1998): 2-3.
[456] Knowles, Malcolm S., Elwood F. Holton III, and Richard A. Swanson. *The adult learner: The definitive classic in adult education and human resource development*. Routledge, 2014.

organised around three fundamental pillars. The *first pillar* emphasises specific levels for university stakeholders. The framework delineates three key stakeholder groups, students, academic staff, as well as administrative personnel, each possessing unique learning requirements and duties under the NDP Act.

Tier 1 – Students (The empowered data subjects)

The objective of this layer is to convert pupils from passive data points into knowledgeable, empowered data subjects capable of exercising their rights. Nonetheless, the foundational Module within the pedagogical interventions comprises a compulsory, non-credit online course during new student orientation, addressing fundamental concepts such as an Introduction to personal data, my rights under the NDP Act, and Methods by which the university utilises students' data[11]. This category includes curricular integration, which entails incorporating data privacy ideas into relevant courses. As an example, a research techniques course will emphasise ethical data collection; a law class will examine the NDP Act; whereas a computer science course will instruct on privacy-by-design principles, among others. To enhance efficiency, the tier includes awareness campaigns including seminars, and readily available materials on the university web that elucidate the process for submitting data access or correction requests.

Tier 2 – *Academic staff of Nigerian Universities (group 1: the data-savvy educators and researcher)*

This component aims to provide lecturers as well as scholars with the expertise to ethically manage student and research data while exemplifying best practices; the pedagogical interventions will include compulsory, discipline-specific training. For an educator, the emphasis may be on student performance metrics; for a medical researcher, the focus may be on managing sensitive health data and executing Data Protection Impact Assessments (DPIAs) for research initiatives. This tier will concentrate on instructional and evaluative training, including responsible utilisation of learning analytics and the creation of tests that reduce privacy infringement. The materials will include user-friendly checklists and templates for executing DPIAs for research, easily accessible via the University's Data Protection Office.

Tier 3 – Academic staff of Nigerian Universities (group 2: the compliant data processors)

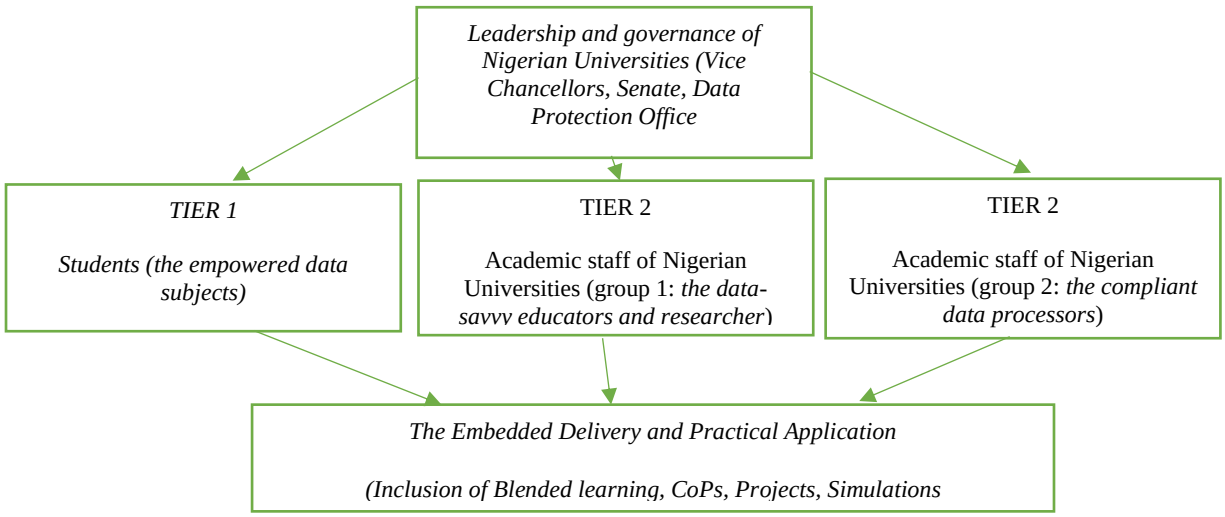
The aim of this tier is to guarantee that personnel in registration, HR, finance, and IT comprehend their essential role as data processors and can execute compliance processes, while the educational intervention will include job-specific training focused on in-depth, procedural instruction for staff managing key operations. The Human Resources department must be familiar with regulations governing worker data processing; the registry must excel in confidential transcript processing; the information technology team must comprehend breach response protocols, including simulations and drills (Conducting table-top activities for a simulated data breach, guiding employees through containment, alerting, and interaction processes as mandated by the NDP Act), and finally, the establishment of explicit guidelines (Creation of detailed, simple Standard Operating Procedures (SOPs) for managing common data requests, such as a student requesting data erasure).

The second pillar

The second pillar emphasises delivery methods and curriculum integration. The Embedded component of the ETAP Framework prioritises integration rather than mere addition. This encompasses blended learning, which employs a combination of compulsory online courses (for basic information) and in-person, experiential classes (for scenario-based problem-solving skills). This facilitates substantial participation while promoting enhanced engagement. Additionally, there exists a component for Communities of Practice (CoPs) that entails the formation of faculty-led and staff-led CoPs, enabling members to exchange difficulties and best practices concerning data privacy in their everyday operations, hence promoting peer-to-peer learning. Finally, the Just-in-Time Learning component emphasises the provision of micro-learning materials, including brief movies that demonstrate complete involvement, as well as media, infographics, as well as FAQs that are readily available when a particular privacy-related inquiry occurs.

Third Pillar – Promotion of the culture of practical application

Theory must be connected to practice in all facets of education to facilitate cultural transformation[457, 458]. This pillar emphasises the development of mechanisms for application. The initiative advocates for the establishment of an annual University-Wide Data Privacy Day, including lectures, simulated data rights clinics, and presentations by NDPC officials to ensure ongoing visibility and involvement. Additionally, the support of student projects and capstone initiatives promotes final-year endeavours that tackle authentic data privacy issues inside the institution, such as evaluating a particular procedure or developing a privacy-conscious application for campus use. Ultimately, the effectiveness of the framework depends on the evident support from university leadership, including Vice-Chancellors and Registrars, as well as the role of incentives in leadership. This entails recognising and rewarding departments that exhibit outstanding data protection measures.



Source: Researchers, 2025

[457] Ojo, O. O., and G. A. Obimuyiwa. "Electronic record-keeping system and administrative effectiveness of polytechnics in Ogun State, Nigeria." *Nigerian Journal of Educational Foundations* 18, no. 1 (2019): 184-193.

[458] Daramola, Dorcas Sola, and Gabriel Ayodeji Obimuyiwa. "Effects Of Manual And Computer-Based Concept Mapping Innovative Strategies On Academic Performance Of Pre-Service Teachers In Kwara State Colleges Of Education." *Epiphany* 15, no. 2 (2023): 118-139

5. Discussion

The proposed framework serves not only as a teaching model but also as a roadmap for a significant cultural transformation inside Nigerian institutions. The implementation has significant ramifications for the administration of universities, regulatory policy, and the fundamental understanding of a contemporary, rights-conscious university in the Global South. The framework's principal contribution is its direct engagement with the significant gap noted in the literature: the divide between compliance with procedures and cultural internalisation. As Solove[12] and several other researchers have argued, legislation alone cannot establish ethical data stewardship. This framework elucidates the previously absent methodology. By using a pedagogical perspective, it transforms data protection from a cumbersome statutory obligation into an essential element of the university's instructional and ethical purpose. This corresponds with Fullan's[18] theory of educational transformation, which asserts that effective reform calls for changes in both resources (policies, instruments) and, crucially, in ideas and behaviours. The tiered structure guarantees that this shift is substantive and throughout the organisational hierarchy, empowering all stakeholders from first-year students to senior administrators.

A primary advantage of the framework is its awareness of its surroundings. It acknowledges the well-documented weaknesses of the Nigerian higher education system, including financial limitations, infrastructural deficiencies, and oversised class sizes[8,11], and instead designs solutions that accommodate these challenges. Blended learning utilises scalable online courses for core information, conserving limited in-person resources for impactful, interactive sessions. The focus on incorporating privacy into current courses, instead than developing new ones, is a practical solution to overloaded curriculum. This methodology makes the framework a feasible foundation, especially for resource-constrained organisations, fostering gradual advancement rather than an unrealistic aspiration. It provides a framework for other industries and nations in the Global South encountering similar issues of fast digitisation amid constrained institutional capability.

Furthermore, the framework explicitly endorses the strategic foundations of the Nigeria Data Protection Commission, especially its dedication to knowledge-based regulation[3]. A university that effectively applies the framework transitions from a prospective location of non-compliance and enforcement to an engaged collaborator in fostering a national culture of data protection. The framework enables colleges to serve as models, cultivating graduates who are not just knowledgeable about their data rights but also prepared to be privacy-aware professionals in the industry. This has a significant multiplier impact, harmonising the university's fundamental aim of knowledge propagation with the national strategic goal of establishing a resilient data ecosystem.

Nonetheless, despite its design, the implementation process is beset with problems that must be recognised, including Leadership Buy-in along with Funding. Initial motivation and ongoing financial support need dedicated university leadership. The anticipated cost of adoption should be evaluated against the concrete and abstract expenses associated with a significant data breach or regulatory penalty. The user must also be prepared to address opposition to change. Resistance is unavoidable in every institutional transformation. Academic personnel may see this as an extra encumbrance, whilst administrators may adhere to antiquated, ineffective practices. Surmounting this requires continuous communication, illustrating the value proposition, and integrating incentives.

Additionally, another potential concern is delivery capacity. Who will create the courses and provide the training? This requires the creation or enhancement of a central Data Protection

Office within the institution, staffed with individuals who have both legal acumen and educational proficiency. This office will serve as the operational hub for the framework's execution. It is essential to evaluate the impact, since the efficacy of the framework cannot be determined just by compliance indicators. Longitudinal metrics are essential, including the monitoring of accurately processed data subject requests, decreases in small internal breaches, and favourable changes in attitudes assessed by pre- and post-implementation surveys. The framework signifies a fundamental transformation. It contends that the greatest lasting safeguard for a university's data is not software, but rather an informed and watchful community. Through the investment in human capital via a systematic educational plan, a Nigerian university may transition from vulnerability to resilience, protecting the rights of its constituents while meeting its responsibilities as a data controller in the age of digitisation.

6. Conclusion and Recommendations

The study contends that the effective execution of the NDP Act in the higher education sector necessitates a fundamental culture shift, which fundamentally represents a pedagogical problem. The transition from basic regulatory compliance to a robust culture of data security needs more than laws and designated officials; it requires a systematic, deliberate, and ongoing educational initiative that involves all stakeholders of the university community. The suggested framework provides a systematic strategy to accomplish this, transcending a techno-legalistic perspective to establish data privacy as a fundamental aspect of the university's instructional purpose and ethical character.

The framework's efficacy is rooted in its acknowledgement of the unique duties and obligations of students, academic personnel, and administrative staff, offering customised learning interventions that are contextually relevant and pragmatically applicable. The framework advocates for integration into current curricular and operational structures, offering a feasible model for the resource-limited Nigerian setting, transforming perceived limitations into possibilities for creative, integrated learning. This approach perceives the NDP Act not just as a compliance obligation but as a stimulus for institutional advancement, digital citizenship, and the development of a rights-respecting academic atmosphere.

Nonetheless, a theoretical framework is simply a first foundation. Its promise can only be actualised via coordinated efforts. This study finishes with specific suggestions for key stakeholders, delineating a clear transition from theory to practice. Nigerian University Administrations, especially Vice-Chancellors and Councils, should lead this cultural transformation from the highest levels. This starts with the official formation and staffing of a central Data Protection Office, entrusted with the power and skills to manage the execution of the framework. University leadership must expressly incorporate data privacy literacy as a strategic aim in institutional growth plans and give dedicated funds for the creation of training modules, seminars, and awareness campaigns. Moreover, promoting interdepartmental communication across ICT units, academic units, and administrative units is essential for achieving a cohesive and consistent strategy.

The Nigeria Data Protection Commission (NDPC) has the chance to use the higher education industry as a model of best practice. The NDPC is advised to create a distinct Code of Conduct for the Higher Educational Sector, which would provide specialised advice on the implementation of the NDP Act in academic settings. The Commission might further serve as a catalyst by recognising and certifying colleges that exhibit exceptional data security cultures, perhaps via an

annual awards system. Furthermore, collaborating with the National Universities Commission (NUC) to include fundamental data protection principles into certification criteria would provide a significant systemic motivation for institutions to allocate resources towards these educational programs.

The paper presents several opportunities for future research for researchers in academia and educational experts. Empirical study is essential to pilot and statistically evaluate the effects of the framework or its elements in certain Nigerian institutions. Research should investigate the establishment of standardised criteria for evaluating data privacy culture, transcending compliance checklists to measure changes in viewpoints, behaviours, and organisational practices. Comparative analyses with other African countries would be essential in establishing a comprehensive understanding of data protection within higher education environments in the Global South. Ultimately, the digitisation of Nigerian higher education is an inevitable and essential advancement. The issue is not whether universities will handle data, but rather if they will do it effectively, ethically, and in a way that protects the basic rights of those they serve. Nigerian universities can enhance their credibility as institutions by accepting their duties as educators in both academic disciplines and technological citizenship, thereby developing graduates who are not just proficient professionals but also knowledgeable and empowered data subjects.

Data Subject Rights: Real World Application of Rights to Access, Rectification, Object, Erasure, and Data Portability

Faith Amarachi Okpara, PhD, ACIS
Bowen University
amarachiokpara01@gmail.com
&
Chinonso Queenesther Emeka

ABSTRACT

This study investigates the practical application and challenges of exercising data subject rights under the General Data Protection Regulation (GDPR 2016/679) in the EU and Nigeria's Data Protection Act (NDP Act, 2023). It emphasises the importance of rights such as access, rectification, objection, erasure, and data portability for data protection, transparency, and trust in digital economies. The research aims to assess awareness and understanding of these rights among individuals and organisations, evaluate the processes and challenges faced by data controllers and processors in handling requests, and identify best practices for effective implementation in line with GDPR and NDP Act requirements. Utilising a mixed-methods approach, the study reveals findings related to awareness levels, implementation challenges, technological limitations, and variability in practices. Recommendations include enhancing capacity building, establishing clear processes, leveraging technology, and fostering regulatory collaboration. Ultimately, the effective realisation of data subject rights is crucial for building trust, ensuring compliance, and promoting data protection in Nigeria and globally, aligning with international standards.

Keywords: Data Subject, Rights, GDPR, NDP Act, Privacy

1. Introduction

The right to privacy, as outlined in Section 37 of Nigeria's 1999 Constitution, has gained importance in the digital age, especially concerning data, which drives technological progress. In the realm of artificial intelligence, the significance of data has led to the acknowledgement and enforcement of data subject rights, allowing individuals to control their personal data, including access, processing, usage, and retention. Regulatory bodies address complaints regarding violations

of these rights, holding data controllers accountable through fines or compliance mandates. However, awareness and exercise of these rights vary, and implementation can be challenging for data controllers, particularly when compliance mechanisms are inadequate. The GDPR defines a data subject as an identifiable person in the EU, while Nigeria's NDP Act similarly defines it as an individual related to personal data.

Data such as the websites an individual has accessed and their language preferences may appear benign; yet, the GDPR categorises them as personal data due to their potential to create a digital footprint that facilitates identification, especially when several data points are aggregated. [459]

2. Data Subject Rights

In a progressively data-centric society, safeguarding personal information has emerged as a critical issue. In acknowledgment of the necessity to protect individual privacy and rights, President Bola Ahmed Tinubu enacted the Data Protection Act, 2023, thereby legislating the establishment of the Nigerian Data Protection Commission, which is empowered to formulate and enforce regulations for the safeguarding and security of personal data of Data Subjects in Nigeria..[460] The new legislation in Nigeria establishes a comprehensive framework for data protection, granting significant rights to individuals over their personal data. This empowers data subjects to control how their information is collected, processed, and shared, while also imposing obligations on data controllers to ensure transparency. Similar rights exist globally, promoting uniformity and common expectations, but there is a call for more regional harmonization, particularly in Africa, to enhance awareness and enforcement. Key rights include access, rectification, objection, erasure, and data portability, which are crucial for building trust in digital economies. Effective implementation of these rights requires organizations to have processes in place to manage requests, ultimately promoting data protection and privacy.

The GDPR delineates eight data subject rights in Chapter III to data subjects and mandates respective obligations to data controllers (and data processors).. The GDPR's data subject rights are as follows: Right to be informed,[461] Right of access[462], Right to rectification,[463] Right to be forgotten,[464] Right to restrict processing,[465] Right to data portability,[466] Right to object to processing,[467] and Rights in relation to automated decision-making and profiling.[468] Giannopoulou et al. categorise the GDPR's data subject rights into two groups according to their mandate, passive

---

* Faith Amarachi Okpara, PhD, ACIS, https://orcid.org/0009-0006-6191-9848, and Chinonso Queenesther Emeka, Senior Associate at Privalex Advisory, chinonsoemeka54@gmail.com.

[459] Celestine Bahr, 'GDPR data subject rights: An in-depth guide with examples' (2025) <https://usercentrics.com/knowledge-hub/gdpr-data-subject-rights/> accessed 20 September 2025.

[460] Iquo Essien, 'The Rights Of Data Subjects Under The Nigeria Data Protection Act: Empowering Individuals In The Digital Age' (2024) <https://thefirmaadvisory.com/new-blog/2024/1/29/the-rights-of-data-subjects-under-the-nigeria-data-protection-act-empowering-individuals-in-the digital age#:~:text=The%20right%20to%20rectification:%20If,data%20to%20be%20deleted%20instead.> accessed 15 September 2024

[461] Articles 12 to 14 of the General Data Protection Regulation of the EU

[462] Article 15, *ibid*.

[463] Article 16, *ibid*.

[464] Article 17, *ibid*.

[465] Article 18, *ibid*.

[466] Article 20, *ibid*.

[467] Article 21, *ibid*.

[468] Article 23, *ibid*.

and active.[469] Passive rights, such as the right to be informed,[470] (Articles 13 & 14), aim to facilitate the exercise of rights. The active rights outlined in Articles 15 to 18 and 20 to 22 of the GDPR, pertain to the entitlements of data subjects. These rights can be categorized by their objectives: Articles 15 and 20 emphasize transparency; Articles 16 and 17 address personal data; and Articles 18, 21, and 22 GDPR focus on data processing. This article specifically discusses the rights to Access, Rectification, Object, Erasure, and Data Portability.

2.1. Right to Access

The right of access, is often the starting point for other requests. For example, it is this same right that facilitates other rights, because it gives the data subject the right to obtain confirmation on whether his or her data are being processed in the first place. If in fact personal data are being processed, then the data subject can have inaccurate data rectified or have incomplete data made complete.[471]

Under the Nigeria Data Protection Act (NDP Act)[472] and the General Data Protection Law (UK GDPR)[473], Data subjects have the right to know if a data controller is processing their personal data under the GDPR. These requests must be processed quickly and without restrictions. Data subjects have the right to detailed information about personal data processing, including its purpose, categories of data, and recipients, including foreign recipients. They should understand the data retention period and its reason.

Data subjects can also request rectification, erasure, or restriction of personal data processing and object to it. They can lodge a complaint with the Data Protection Commission. If the data was not collected directly from the person, the organization must disclose its source. Organizations must explain the effects of automated decision-making or profiling on individuals. Data subjects can obtain a copy of their personal data in a common electronic format, however companies may charge if the request is unreasonable. This is a data subject access request. Companies must reply to Data Subject Access Requests (DSARs) within 30 days, with a 30-day extension for difficult requests. Organisations may refuse excessive or unnecessary DSARs, but they must show evidence, requiring careful review. The European Data Protection Board (EDPB) gives recommendations on identifying excessive or unjustified requests to efficiently process data subject enquiries.

2.1.1. Real World Applications of the Right to Access

The Information Commissioner's Office (ICO) in the UK regulates data protection and administers the Data Subject Access Request (DSAR) framework, which allows individuals to access their personal data held by organizations. This right is recognized internationally in various data protection laws. The ICO recently reprimanded the Labour Party for failing to respond to

---

[469] Giannopoulou A., Ausloos J., Delacroix S., & Janssen H., 'Intermediating data rights exercises: The role of legal mandates', *International Data Privacy Law* (2022) <https://doi.org/10.1093/idpl/ipac017> accessed 8 September 2025.
[470] A.A. Habu and T. Henderson, 'Data subject rights as a research methodology: A systematic literature review', *Journal of Responsible Technology* (2023) 16, 100070, 3.
[471] 'GDPR & Data Protection Consultant' <https://www.gdprxpert.ie/right-to-rectification-and-principle-of-accuracy/?utm>, accessed August 14th 2025.
[472] Section 34 Nigeria Data Protection Act 2023
[473] (n 4).

Subject Access Requests (SARs) following a 2021 cyberattack that led to an influx of requests. Between November 2022 and early 2024, 78% of 352 SARs were not addressed within the mandated three-month period, with over half delayed by more than a year. Additionally, a "privacy inbox" was found to contain 646 unanswered SARs and 597 deletion requests dating back to November 2021. The ICO highlighted the importance of timely responses for maintaining transparency and trust, particularly in political contexts, following over 150 public complaints. The 2021 cyber incident was believed to be a ransomware attack that made significant amounts of member and supporter data inaccessible.[474]

The case of *Harrison Kisaka v. Faulu Microfinance Bank Limited*[475] concerned the alleged infringement of Kisaka's rights as a data subject under Kenya's Data Protection Act, 2019. The bank declined to disclose Kisaka's negative background check report, which revoked his banking application for privacy reasons. Active criminal actions against Kisaka, who claimed the material was his personal data and that the bank's refusal of access violated his rights, underpinned the report. The Data Protection Commissioner found that Kisaka's right to view and update his personal data was breached in the report, per Section 26 of the Data Protection Act. Faulu Microfinance Bank violated transparency rules by omiting to disclose Kisaka's personal data and its origin, according to the Commissioner. This case highlights key provisions of the Data Protection Act, including data subjects' rights to access their data, data controllers' duties to operate correctly and transparently, and data management privacy policies. It stresses that data protection standards regulate recruitment-related background checks, protecting candidates' rights to know and access their personal data. The bank had seven days to comply with Kisaka's request or face action.[476]

The right to access personal data is a legal obligation for data controllers, not merely a privilege. They are required to furnish clear, timely, and accurate information upon request, which empowers individuals to make informed choices regarding their data and to address any potential misuse. This obligation is essential for fostering trust between organisations and the individuals whose data they handle.

2.2. The Right to Rectification

Article 16 of the General Data Protection Regulation (GDPR) articulates the right to rectification with improved clarity and power. This right is often construed with GDPR Article 5(1)(d) accuracy. As an individual data protection principle, accuracy is only stated in the text. It works with all the other principles to form a whole. Article 5(1)(d) requires personal data to be "correct and, when necessary, up-to-date; all reasonable measures must be taken to erase or rectify inaccurate personal data for the purposes for which they are processed."[477]

---

[474] Jessica Elgot , "Labour failed to respond on time to People's request for data. Say ICO". *The Guardian*, (August 28 2024) <https://www.theguardian.com/politics/article/2024/aug/28/labour-failed-to-respond-on-time-to-> accessed 16 August 2025.

[475] (ODPC Complaint No. 0586 of 2023)

[476] Case Law Library, *Harrison Kisaka v. Faulu Microfinance Bank Limited*, <https://caselawlibrary.cipit.org/cases/detail/Harrison%20Kisaka%20-vs-%20Faulu%20Microfinance%20Bank%20Limited#> accessed 18 September 2025.

[477] GDPR & Data Protection Consultant <https://www.gdprxpert.ie/right-to-rectification-and-principle-of-accuracy/?utm> accessed 12 September 2025.

The General Application Implementation Directives 2025 of the Nigeria Data Protection Act mandate that data controllers and processors must facilitate effective data rectification processes without requiring affidavits or newspaper publications, particularly when aligning data with a subject's National Identification Number (NIN). If an error in personal data entry is made by the data controller or processor, the data subject should not incur costs for rectification. Furthermore, it is essential that data subjects are given sufficient opportunities to verify their data prior to its permanent submission. In cases of disputes regarding the adequacy of these verification opportunities, the onus is on the data controller or processor to provide evidence of compliance. Accordingly, data processing platforms together with technical and organisational measures for their operations shall be designed in a way that may allow a data controller or data processor to audit any source of data error"[478] A data subject may request an organization to rectify or update their information if they discover inaccuracies or omissions in the data held about them. This right is essential due to the dual nature of correctness, which can be both subjective and objective. For example, if a data subject marries or alters their name, they may request the organizations to amend their information accordingly. This right is of equal significance to other rights under the Nigeria Data Protection Act (NDP Act). In circumstances where rectifying inaccurate, incomplete, or misleading data is unfeasible, the NDP Act permits the deletion of such data instead. Section 34(c) of the NDP Act 2023.

According to the UK GDPR, "the data subject has the right to promptly obtain rectification of inaccurate personal data from the controller." The data subject has the right to complete incomplete personal data, including by the provision of a supplementary statement, in light of the processing purposes.[479].

2.2.1. Real World Applications of the Right to Rectification

In Case C-247/23, adjudicated by the Court of Justice of the European Union (CJEU) on March 13, 2025, the court addressed the case of VP, an Iranian transgender refugee in Hungary, whose gender was inaccurately recorded as female in the national asylum register despite medical documentation affirming his male identity. The Hungarian asylum authority had denied VP's request for rectification under Article 16 of the General Data Protection Regulation (GDPR), citing the necessity of proof of gender reassignment surgery. The CJEU determined that EU member states are prohibited from denying the rectification of inaccurate gender data in public registers based on the absence of a national gender recognition procedure or the requirement of surgical intervention. The court emphasized that while "relevant and sufficient" evidence may be necessary, a medical or psychological certificate satisfy this, and any restrictions must comply with Article 23 GDPR. Drawing on Article 8 ECHR, the court stressed that gender identity is a core element of private life, and recognition cannot depend on surgical treatment. The decision underscores that GDPR rights, including rectification, take precedence over restrictive national practices and extend to deeply personal identity data[480].

---

[478] Article 36 of the General Application and Implementation Directives 2025
[479] Article 16 GDPR
[480] Etienne Drouard and others, (2025) <https://www.hoganlovells.com/en/publications/gender-and-gdpr-does-the-right-to-rectification-override-civil-registry> accessed 18 September 20255

The right to rectification is a crucial mechanism for safeguarding the integrity and reliability of personal data managed by data processors and controllers. It enables individuals to request corrections to inaccurate or incomplete information, thereby enhancing the accuracy, relevance, and fairness of data processing activities. This right not only fosters transparency and accountability but also ensures that decisions—whether automated or human—are based on accurate and current information, mitigating risks of harm, discrimination, or unfair treatment. Ultimately, it bolsters trust between data subjects and data handlers, promotes adherence to data protection regulations, and facilitates improved decision-making in both public and private sectors.

2.3. The Right to Object

Data subjects possess the right to contest the processing of their personal data. In response to such an objection, the data controller is required to cease processing unless they can provide evidence of a public interest or other legitimate reasons that take precedence over the data subject's rights and interests. In cases where personal data is processed for direct marketing including related profiling the data subject may object at any time, and once such an objection is made, the personal data must no longer be processed for direct marketing purposes[481].

Under the UK GDPR, data subjects possess the right to object to the processing of their personal data under specific circumstances. Notably, individuals can object to the processing of their data for direct marketing purposes at any time. Additionally, objections can be raised concerning the processing of personal data for scientific or historical research, unless such processing is essential for fulfilling a task in the public interest. This right is not absolute, you can refuse to comply if you demonstrate compelling legitimate grounds which override the interests of the individual, or the processing is for the establishment, exercise or defense of legal claims[482].

2.3.1. Real World Application of The Right to Object

In a significant legal case highlighted by the Guardian on March 25, 2025, Tanya O'Carroll, a human rights advocate from London, contested Meta (the parent company of Facebook) regarding the General Data Protection Regulation (GDPR) and the right to object to personal data processing. O'Carroll raised concerns about Facebook's inference of sensitive information, including her familial connections, financial situation, and political beliefs, based on her online behavior. She exercised her absolute right to object to such processing, which is free under the law. Four years later, just before trial, Meta agreed for the first time to stop targeting ads to a user based on their personal data marking a significant victory for individual privacy rights and enforcement of the GDPR[483].

---

[481] (n 20)
[482] (n 9)
[483] Dominic Grieve, 'One brave woman wrenched back control of her data from tech giants' <https://www.theguardian.com/commentisfree/2025/mar/25/control-personal-data-tech-giants-meta> accessed 2 August 2025.

2.4. Right To Erasure or Right To Be Forgotten

This right is provided under the NDP Act[484] and the UK GDPR[485] The right to erasure is also known as 'the right to be forgotten'.

The data subject possesses the right to request the erasure of personal data from the data controller under specific conditions, including the withdrawal of consent, the irrelevance of data for its original purpose, unlawful processing, objection to processing, or compliance with legal obligations. However, this right is not applicable in certain circumstances, such as when data processing is mandated by law, for public interest archiving, for legal claims, or for public health reasons. If a valid erasure request is made and no exemptions are applicable, the controller must ensure that the data is erased from both active and backup systems.

2.4.1. Real World Applications of the Right to Erasure or Right to be Forgotten

The Irish Data Protection Commission (DPC) addressed a case involving a complaint under Article 17 of the General Data Protection Regulation (GDPR), which pertains to the right to erasure. A complainant sought the removal of personal data linked to a negative online review about their workplace. Initially, the data controller denied the request, prompting the complainant to escalate the issue to the Spanish Data Protection Authority (AEPD), which subsequently transferred the case to the DPC as the Lead Supervisory Authority. Following DPC intervention, the data controller reconsidered and ultimately removed the review, illustrating the DPC's effective resolution process in facilitating individuals' rights under GDPR.

Additionally, a report by The New York Times on October 3, 2014, highlighted Google's compliance with the European "right to be forgotten" by removing links to five articles from its search results in Europe. Among the removed articles were personal announcements and a report involving reputational concerns, despite their factual accuracy. Since the European Court of Justice ruling in 2014, Google has received approximately 140,000 requests for link removals, approving around 50% of them. This situation has also impacted various European media outlets, with instances of reinstatement of links following publisher challenges.

The report highlights the ongoing tension between privacy rights and freedom of expression, noting Europe's approach of balancing both rights, in contrast to the U.S., where freedom of expression is strongest.[486].

2.5. Right To Portability

Under the UK GDPR[487] The data subject is entitled to obtain their personal data, which they have supplied to a data controller, in a structured, commonly used, and machine-readable format (such as CSV, XML, or JSON) under two conditions: when the processing is based on consent and when

---

[484] Section 34(2) Nigeria Data Protection Act 2023.

[485] (n 6)

[486] Noam Cohen and Mark Scott, " Times Articles remove from Google Results in Europe" *New York Times,* (2014) <https://www.nytimes.com/2014/10/04/business/media/times-articles-removed-> accessed 8 August 2025.

[487] (n 8)

it is conducted through automated means. Additionally, the data subject has the right to request the direct transmission of their personal data from one controller to another.

This right will not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

Looking at the provision of the NDP Act,[488] The Commission is empowered to establish regulations regarding the right of personal data portability, which allows data subjects to obtain their personal data from data controllers in a structured, commonly used, and machine-readable format without undue delay. This right also enables data subjects to transfer their data to another data controller without obstacles and, where feasible, to facilitate direct transfers between controllers. The Commission may define the conditions under which this right can be exercised and outline the obligations for data controllers and processors, particularly concerning costs and timing.

2.5.1. Real World Application of The Right to Portability

The International Association of Privacy Practitioners (IAPP) reports that the EU General Data Protection Regulation (GDPR) established the right to data portability under Article 20, aimed at enhancing individual control over personal data and facilitating the transition between digital services. This right is limited to personal data provided by the data subject, processed based on consent or contract, and handled through automated means. The intention was to mitigate vendor lock-in, particularly in digital consumer services.

However, a survey by Lex Mundi Network across the 27 EU member states indicates minimal progress in supervisory enforcement or case law related to data portability, with most jurisdictions reporting little activity. Noteworthy national interpretations include Lithuania's inclusion of full banking histories, France's acknowledgment of purchase history, and Spain's broader right to "content portability" for social media. Key judicial rulings, such as those from Amsterdam concerning Uber and Ola Cabs, clarified the requirements for "machine-readable" formats. Despite its potential, the right to data portability is underutilized and offers limited practical benefits, as highlighted by the European Commission's 2020 evaluation of the GDPR. Ongoing disputes regarding the definition of "data provided by" have emerged, with the European Data Protection Board (EDPB) advocating for a broader interpretation than the European Commission. Practical challenges, such as the presence of mixed datasets containing non-personal data or data about third parties, further diminish its effectiveness. The IAPP report suggests that unless reformed, Article 20 is unlikely to achieve its intended consumer empowerment goals.

Future relevance may depend on legislative developments like the proposed European Data Act, which could adopt a broader consumer protection approach and make the GDPR's portability provisions largely redundant by granting both consumers and businesses greater rights to access and transfer data generated through the products and services they use[489]

---

[488] Section 38 NDP Act

[489] Jurre Resus and Nicole Bilderbeek, 'Data Portability in the EU: An Obscure data subject right' *International Association of Privacy Practitioners*, (2022) <https://iapp.org/news/a/data-portability-in-the-eu-an-obscure-data-subject-right/?>, accessed August 15 2025

To exercise data subject rights, three steps are involved,[490] The process for accessing personal data held by data controllers involves three key steps. First, one must identify the relevant data controller. Second, a formal request for data must be submitted, which the data controller is obligated to address unless specific exceptions apply. If a request cannot be fulfilled, the data controller is required to provide a rationale. Lastly, it is essential to engage in correspondence with the data controllers and analyse their responses, as there may be instances where no data is provided, such as in cases of data deletion, legal restrictions, or non-compliance by the data controller.

3.0. Findings of the Study

There are varying levels of awareness regarding data subject rights among individuals and organisations. Organisations encounter implementation challenges, such as efficiently processing requests, ensuring transparency, and balancing rights with other obligations. Common issues include difficulties in identifying personal data, and practices for handling data subject rights vary across different sectors, organisation sizes, and jurisdictions. Additionally, resource limitations, particularly for smaller organisations, hinder their ability to manage data requests effectively due to constraints in time, manpower, and finances. The complexity of locating and processing personal data within extensive and often poorly documented data systems

4.0. Conclusion and Recommendations

The General Data Protection Regulation (GDPR) and the Nigeria Data Protection Act (NDP Act) aim to empower individuals regarding their personal data. Data subjects are entitled to clear information about the processing of their data, including the purpose, duration, and methods used. They possess rights to withdraw consent, request modifications or erasure of their data, and transfer it to another controller. Organizations must establish effective procedures for addressing data subject rights requests, which is not only a legal requirement but also essential for maintaining trust. Training for staff involved in data processing is critical, as they often serve as the initial point of contact for data subjects. Protecting data subject rights is fundamental to safeguarding personal information in the digital realm, akin to physical security measures in the real world. Increased awareness and enforcement of these rights are necessary to promote privacy and foster trust in digital environments.

The outlined strategies emphasise the importance of enhancing capacity building, establishing clear processes, and fostering regulatory collaboration in data protection practices. Key recommendations include:

1. Capacity Building: Organizations should improve awareness and training regarding data subjects' rights and compliance requirements.

2. User-Friendly Processes: Develop transparent procedures for managing data subject requests (DSRs) to facilitate user engagement.

---

[490] Ausloos J., & Dewitte P., 'Shattering one-way mirrors - data subject access rights in practice', *International Data Privacy Law,* (2018) 8(1), 4–28 <https://doi.org/10.1093/idpl/ ipy001> accessed 17 September 2025.

3. Regulatory Collaboration: Encourage cooperation among data protection authorities and stakeholders to create harmonised compliance approaches.

Additional recommendations focus on technological investments and procedural standardisation:

- Specialised Tooling and Automation: Implement technology to automate data discovery and management processes, thereby increasing efficiency in handling DSRs.

- Clear Privacy Notices: Ensure privacy notices are accessible, up-to-date, and compliant with GDPR requirements, detailing data collection practices and user rights.

- Standardised Procedures: Establish repeatable processes for all stages of the DSR lifecycle to ensure consistency and compliance.

- Periodic Training: Conduct regular training across departments to promote a culture of data protection awareness.

- Data Protection Officer (DPO): Appoint a DPO to provide expert guidance on DSR handling.

- Accountability Framework: Develop formal documentation outlining roles and responsibilities related to DSR management.

- Data Mapping: Implement data mapping to enhance data management and facilitate quicker responses to DSRs.

- Regular Audits: Conduct audits to assess the efficiency of DSR handling and identify areas for improvement.

- Key Performance Indicators (KPIs): Monitor metrics related to DSRs to evaluate effectiveness and drive continuous improvement.

- Feedback Mechanisms: Analyze metrics and gather feedback from data subjects to refine procedures and enhance compliance and user satisfaction.

- Consent Management Software: Invest in specialized software to streamline privacy compliance and adapt to evolving regulations.

These strategies collectively aim to improve data protection practices, ensuring compliance and enhancing user trust.

Privacy by Design and Default: Integrating Privacy Principles into Systems, Services, AI Models and Digital Infrastructure

Baba Dala Fika, SAN
Managing Partner, Baba Dala, SAN & Co
babadalafika@yahoo.com
&
Yusuf Hassan Jonga, Esq. LL.M
Senior Associate, Baba Dala, SAN & Co
jonga.yusufh@gmail.com

ABSTRACT

Since the concept of privacy by design was originally developed by the Information and Privacy Commission of Ontario, Canada; the Dutch Data Protection Authority; and the Netherlands Organization for Applied Scientific Research in a collaborative project in 1995, the rapid advancement of technologies like Artificial Intelligence (AI) Models and various digital infrastructure has made it paramount for privacy to be incorporated into data systems and technologies from the system development phase. The protection of privacy rights has become integral to organisational priorities, project objectives, design processes, and planning operations. As trust in how companies handle data continues to waver, organisations must prioritise preserving data subjects' freedom of choice and control over their data as a core component of their data protection strategy. These closely connected principles of privacy by design (PbD) and privacy by default (PbDf) constitute central obligations in modern data protection regimes codified in the General Data Protection Regulations (GDPR), Nigeria Data Protection Act 2023 (NDP Act) and the General Application and Implementation Directive (GAID) 2025.

This paper analyses the conceptual foundations, legal framework, and practical integration of privacy principles into digital systems, AI models, and large-scale digital infrastructures. It evaluates the importance of PbD and PbDf as not merely legal requirements but a corporate privacy strategy that enhances consumer trust and reduces compliance risks. Ultimately, this paper advocates that embedding these principles across AI models and technological ecosystems from the start is beyond essential and an organisational priority under data protection laws, and recommends the need to establish practices that ensure data protection from the outset.

Keywords: Privacy, Design, Artificial Intelligence (AI), Digital Infrastructures, Governance

1. Introduction

The digital era has ushered in unprecedented opportunities for innovation in emerging technologies like AI and interconnected digital infrastructures. With the deployment of AI in critical applications, making AI systems trustworthy is of prime importance to ensure that they are safe and remain aligned with respect to fundamental rights and societal values.[491] To mitigate such risks, the already existing concepts of privacy by design and privacy by default have emerged as cornerstones of modern data protection law. The EU GDPR, under Article 25, codifies these concepts, while the NDP Act, 2023 and the (GAID), 2025 similarly provides for them. As emerging technologies like AI and machine learning etc., all involve extensive data gathering and analysis, the privacy by design approaches promise to address new challenges as these technologies advance.[492] This growth will entail promoting privacy-friendly technology, fostering collaboration between engineers and privacy experts by developing specific engineering guidelines through workshops and public presentations, and finally focusing on designing and operating IT systems for processing personal data.[493] In theory, PbD calls for a "holistic and rigorous" approach to data protection, involving coordination of multiple parties in its deployment to ensure its effectiveness.[494]

This paper explores the foundational concepts and practical integration of these principles into systems, services, AI models, and broader digital infrastructure.

2. Conceptual Framework

a) Privacy by Design (PbD): Privacy by design is "the philosophy and methodology of embedding privacy into the design specifications of information technologies, business practices, and networked infrastructures as a core functionality".[495] In essence, the product has default consumer-oriented privacy controls and settings that provide appropriate levels of privacy, without placing undue burden on the consumer.[496]

b) Privacy by Default (PbDf): The GDPR contextualised PbDf and provided that "a controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. "[497]

The concept of privacy by default stated in article 25 para 2 of the GDPR ensures that personal data is processed with the highest privacy protection. By default, personal data isn't made accessible to an indefinite number of persons and only personal data that is

---

[491] Roman Hamon, Henrik Junklewitz, Josep Soler Garrido, and Ignacio Sanchez, "Three Challenges to Secure AI Systems in the Context of AI Regulations." IEEE ACCESS 12:61022–61035. <https://doi.org/10.1109/ACCESS.> 2024
[492] What Is Privacy-by-Design and Why It's Important? IEEE Digital Privacy https://digitalprivacy.ieee.org/publications/topics/what-is-privacy-by-design-and-why-it-s-important/
[493] Mevre Tunca, Privacy by Design: "A Systematic Literature Review of European and British Regulatory Perspectives for Software and Information Engineering," *13th International Conference on Software and Information Engineering (ICSIE)* 2024
[494] Liane Colonna, "Addressing the Responsibility Gap in Data Protection by Design: Towards a More Future-oriented, Relational, and Distributed Approach" (2022) 27(1) Tilburg Law Review pp. 1–21. DOI: https://doi.org/10.5334/tilr.274
[495] Ann Cavoukian, "Privacy by design in law, policy and practice: A white paper for regulators, decision- makers and policy-makers," 2011.
[496] International Organization for Standardization. ISO/DIS 31700(En), Consumer Protection, Privacy by Design for Consumer Goods and Services. <https://www.iso.org/obp/ui/#iso:std:iso:31700:dis:ed-1:v1:en> 2023
[497] Article 25, General Data Protection Regulation (Regulation (EU) 2016/679)

necessary for a specific reason shall be obtained. The principles of data minimization and purpose limitation relate to the concept.[498]

c) Data Controller: The NDP Act[499] defines data controller as:

> "An individual, private entity, public Commission, agency or any other body who, alone or jointly with others, determines the purposes and means of processing of personal data."

d) System Development Life Circle: A system development life cycle (SDLC) is essentially a project management model. It defines different stages that are necessary to bring a project from its initial idea or conception all the way to deployment and later maintenance.[500]

3. Theoretical Concept

The relevance of Cavoukian's foundational principles of PbD is evident in the numerous policies that have been developed and approved, integrating this approach. These policies include but are not limited to regulations such as the European General Data Protection Regulation (GDPR), 'Privacy and Data Protection by Design – From Policy to Engineering' by the European Union Agency for Network and Information Security (ENISA) (2014), which emphasize the importance of PbD. Also, international standards such as Consumer Protection: Privacy by Design for Consumer Goods and Services (ISO/DIS 31700) (International Organization for Standardization, 2023) and our very own NDP Act, 2023 and the (GAID), 2025 also support the implementation of PbD principles.[501]

The Foundational Principles of PbD and PbDf and the importance of incorporating the same through the development phases of systems and technologies cannot be overstated. The seven principles are as follows:

i. Proactive, Not Reactive; Preventive, Not Remedial

A privacy-first attitude supports a preventative approach to privacy. Instead of reacting to privacy risks or invasions when they happen, companies will actively build processes and procedures to prevent them from occurring in the first place.[502]

ii. Privacy as the default setting

The collection of personal information must be fair, lawful and limited to that which is necessary for the specified purposes. Wherever possible, identifiability, observability, and linkability of personal information should be minimized.

---

[498] Daniela Ježová, "Principle of Privacy by Design and Privacy by Default," <DOI: https://doi.org/10.18485/iup_rlr.2020.ch10> 2020

[499] s. 65, Nigerian Data Protection Act, 2023.

[500] Anshu Bansal, "7 Phases of the System Development Life Cycle Guide" <https://www.clouddefense.ai/system-development-life-cycle/>

[501] Cristina Del-Real, Els De Busser & Bibi van den Berg, "A systematic literature review of security and privacy by design principles, norms, and strategies for digital technologies, International Review of Law, Computers & Technology," 39:3, 374-405, DOI: 10.1080/13600869.2025.2457227

[502] Kadi Coult Wharton, "The 7 principles of privacy by design" <https://www.onetrust.com/blog/principles-of-privacy-by-design/> 2024

Such default settings include:

Collection limitation: You only collect the amount and types of data you're legally allowed to.

Data minimization: You collect only the absolute minimum amount of data necessary. You won't collect data just for the sake of collection or because you can.

Use, retention & disclosure limitation: You won't use the collected data for any purpose other than that to which the user has agreed. You won't keep data after it's no longer needed for the purposes you stated to users, and you won't disclose the data unless necessary to achieve the purpose for which it was collected.

Security: You implement appropriate technical and organizational measures, such as encryption, to ensure the confidentiality, integrity, and availability of the personal data.

iii. **Privacy embedded into design**

Privacy is embedded into the design of business processes, technologies, operations, and information architectures in a holistic, integrative and creative way. When you plan for privacy at the start of a project, you can incorporate these controls seamlessly, with less cost and effort and more functionality.

iv. **Full functionality-positive-sum, not zero-sum**

Accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made.

v. **End-to-end security Full life cycle protection**

Privacy must be continuously protected across the entire life-cycle of the personal data. There should be no gaps in either protection or accountability. The security has special relevance here because without strong security, there can be no privacy

vi. **Visibility and transparency**

PbD seeks to assure all stakeholders of independent verification. Its component parts and operations remain visible and transparent, to both users and providers alike.

vii. **Respect for user privacy**

Above all, PbD requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.[503]

4. Legal Framework

i. General Data Protection Regulations (EU)

Article 25 of the GDPR explicitly requires controllers to implement PbD and PbDf through technical and organisational measures. It requires controllers to adopt appropriate technical and

[503] Ann Cavoukian, "Privacy by Design, the 7 Foundational Principles, Implementing and Mapping of Fair Information Practices." <https://iapp.org/media/pdf/resource_center/Privacy%20by%20Design%20 - %207%20Foundational%20Principles.pdf>

organisational measures in considering the development, implementation costs, nature, scope and purposes of processing. This is to be considered with the risks to data subjects' rights when determining processing methods and during processing. These measures must effectively embody data-protection principles such as pseudonymisation or data minimisation; and embed the necessary safeguards to ensure compliance and protect data subjects. Recital 78 of the GDPR further reinforces Controllers to ensure that, by default, only personal data necessary for each identified purpose is processed. This requirement governs the volume of data collected, the extent of processing, the duration of storage and the degree of accessibility. By default, personal data must not be accessible to an unrestricted number of persons without the individual's involvement.[504]

Today, in order to comply with the requirements of Article 25 of the GDPR, as well as to avoid large fines, every online business must analyse how, where, and when the personal data of users is processed, and also ensure that one of the main human rights, 'the right to privacy life' was taken into account at every stage of processing, starting from the initial design phase.[505]

II. NDP Act General Guidelines or Application and Implementation Directive, 2025

Article 31 of the GAID provides guidelines for the Deployment of a Data Processing Software by a Data Controller or Data Processor, its states that:

> "(2) For the purposes of complying with this GAID and in addition to other obligations imposed on a data controller or a data processor, it is mandatory for the data controller or data processor in the circumstances referred to in Article 31 (1) to:
>
> a) Carry out a DPIA before the deployment of the software;
>
> b) Ensure that the software is designed in accordance with the *principles of privacy by design and by default;"*

Article 43 (2) f also provides that:

> "(2) A data controller or a data processor who deploys or intends to deploy Emerging Technologies (ETs) for the purposes of processing personal data is expected to set forth technical and organisational parameters for the processing in order to design its ET tools in accordance with the threshold of data processing permitted by law, particularly taking into account the:
>
> f) Privacy by design and by default."[506]

In essence, to build a privacy-aware IoT (Internet of Things) application that complies with the rules of privacy and data protection laws, software developers need to deal effectively with the legal aspects of it, understand its provisions, and translate these legal requirements into technical requirements that are applicable to the technical domain.[507]

---

[504] General Data Protection Regulations (EU) <https://gdpr-info.eu/art-25-gdpr/>
[505] Violetta Loseva, Serhii Floreskul, "Privacy by Default and by Design"< https://avitar.legal/blog/privacy-by-design-and-by-default> 2024
[506] Nigeria Data Protection Act (NDP Act) 2023-General Application and Implementation Directive (GAID) 2025
[507] Aljeraisy, Atheer, Masoud Barati, Omer Rana, and Charith Perera. "Privacy Laws and Privacy by Design Schemes for the Internet of Things: A Developer's Perspective." A*CM Computing Surveys 54 (5): 1–38* 2022., <https://doi.org/10.1145/3450965>

5. System Development Life Cycle

Based on the seven foundational principles articulated by Ann Cavoukian and their codification in data protection laws such as the GDPR and the NDP Act, it is essential to outline the stages of system development in relation to the corresponding privacy requirements. While different teams might implement SDLC methodology in different ways, practitioners broadly agree that the software development lifecycle has seven key phases, viz[508]:

i. Planning Stage

The project planning phase establishes the goals and scope of a software development project. The software development team starts by brainstorming high-level project details. The team focuses on ideas such as the problem the software will solve, who will use it and how the software might interact with other applications and systems. The planning phase often produces an initial software requirement specification (SRS) document detailing the details of software's functions, required resources, possible risks and project timeline.

ii. Analysing Stage

During the analysis phase, the development team collects and analyzes information on the project's requirements. Analysis often involves gathering user requirements, conducting market research and feasibility testing, evaluating prototypes and allocating resources.

iii. Design Stage

The design phase involves defining the project's architecture. Core steps include outlining the software's navigation, user interfaces, database design and more. They consider how the software fits into an organization's existing landscape of apps and services. The development team might also begin to address cybersecurity concerns during the design phase by using threat modeling exercises to identify potential risks for the software which culminates in the creation of an early prototype or multiple prototypes. Design phase work is collected in a software design document (SDD), which is passed on to developers as a roadmap to use while coding.

iv. Coding Stage

The coding phase, or development phase, is when the team starts writing the code and building the software, based on the SDD, SRS and other guidelines created during the preceding phases. These documents help guide software developers in choosing the correct programming language, such as JavaTM or C++, and they help project managers divide the project into smaller, discrete coding tasks.

This phase also involves building any additional systems or interfaces necessary for the software to function properly, such as web pages or application programming interfaces (APIs).

v. Testing Stage

The testing phase begins after the development team has created a functional piece of software. During this phase, the team looks for opportunities to eliminate bugs and enhance the final

[508] Gita Jackson, Matthew Kosinski, Jim Holdsworth, "What is the software development life cycle (SDLC)?" <https://www.ibm.com/think/topics/sdlc> 2025

product. Quality assurance tests help ensure that the software meets user and business requirements and works within the organization's broader IT environment.

vi. Deployment Stage

In the deployment phase, finely tuned software is deployed to the production environment where users can access it. The goal of this phase isn't just to get the software into the hands of users. Developers want to make sure that users understand how to use the new software, and that it can be deployed with minimal disruption to user experience or workflows.

vii. Maintenance Stage

The SDLC doesn't end when the software is deployed. The maintenance phase entails the post deployment work that software teams do to help ensure the software's continued operation by pushing updates and optimizations, making unanticipated changes, testing patches, addressing new use cases and squashing any bugs that users find.

Also, ongoing maintenance and support are necessary to safeguard the longevity of any piece of software. This is reinforced in **Article 29** of the NDP Act-GAID, which requires data controllers or data processors to have schedules for monitoring, evaluation and maintenance of data security systems.

6. Integrating Privacy Principles into Systems, Services, AI Models and Digital Infrastructure.

It is important to understand that PbD takes a design thinking approach to managing individual control over personal data flow, incorporating it into systems and technologies by default. People generally treat this as an 'engineering issue', however, it is believed to be a strategy that needs to be implemented at base level. These are some of the strategies[509]:

Apply the seven principles during scoping and planning

When it comes to personal data, there should be a 'less is more' approach. The scoping team should clearly identify and define the data elements that would be gathered through the product. For any user story or epic involving data collection, a clear description of both the collection's purpose and the data's subsequent use is required. These aspects will ensure that developers and architects understand and appreciate the sensitivity and purpose of the information collected from users and enable them to incorporate the relevant safety measures in subsequent development phases.

a) Embed security throughout the data life-cycle

Data collected by software is not only varied and expansive in nature, but may also have a very long life cycle. Therefore, the core principles of PbD should apply at each juncture of data generation, transformation and usage and deletion where necessary.

b) Application and Software Data Protection Impact Assessment

---

[509] Sonali Saraswat, Karthik Venkata and Dhritimaan Shukla: Pwc: "Understanding and implementing privacy by design in software development." <https://www.pwc.in/assets/pdfs/consulting/cyber-security/data-privacy/understanding-and-implementing-privacy-by-design-in-software-development.pdf > 2021

An application and software data protection impact assessment (DPIA) helps developers to identify, analyse, and explain how an application impacts the privacy rights and freedoms of its users. A DPIA should be performed against applications intending to collect, maintain, and/or share personal information. By embedding a DPIA early within the software development lifecycle, developers are able to mitigate unacceptable privacy risks and resolve GDPR user privacy rights compliance issues before the completion of the application's design.[510] Section 28 of the NDP Act and Article 28 (2), (3) f and g of the GAID provides for mandatory DPIA on new technologies and the development of software.

c) Monitor the product's data sinks

Software's and AI models tend to collect information that either (a) it is not meant to collect, or (b) that is in addition to the information that it is tasked to collect from the user. Hence, it is wise to perform regular and periodic checks on the data sinks of the software.

d) Reinstate user autonomy over personal data through privacy controls

Before collecting information, inform users about why or for what purpose their data is being collected, how their data is being stored and protected, and for how long the organisation or software will store the data. It is also important to create a user-friendly privacy policy and not a long-drawn legal document. More importantly, update users about changes to the policy. This is because data privacy laws and norms are constantly changing, and hence, a software application's privacy policy would require additional clauses or modifications. Such changes can be compiled in an email or a document and sent to relevant users. This need not be a manual process, and a mechanism within the software can be used to enable such communication to the user. Each change to the privacy policy should be followed by seeking implied and informed consent from the user, before submission of data or transacting with the software.

e) Run analytics to identify data leeches

Product owners should monitor the data pipeline (data at rest and in transit) to identify programs, trackers and bots that are 'feeding' on the information contained in the software. While encryption can protect the data from being misused, periodically analysing data traffic can serve as an added layer of privacy protection.

f) Minimise data access to support teams

While designing software, the role of support personnel should be critically considered. Support teams such as database admins, network support and DevOps support should not be provided access to user data, either from the front end or in the data layer. Obfuscation and anonymisation controls can be used for the log-ins provided to the support teams. Even if a task requires the support personnel to peek into the data, private information can be masked on the UI. Changing encryption keys also mitigates privacy breaches via backdoors that are typically used by internal aggressors.

These strategies can also be embedded into AI models, which tend to rely heavily on large datasets, often involving personal or sensitive data. Their effective implementation makes a major

[510] Dave Whitelegg, "GDPR - Application privacy by design: Explore guidance designed to help you develop applications that are compliant with the European Union's GDPR." <https://developer.ibm.com/articles/s-gdpr2/> 2024

contribution to both securing the rights of individuals and enhancing the credibility of businesses.[511]

7. Prospects of Integrating Privacy Principles into Systems, Services, AI Models and Digital Infrastructure.

i. Protection of the user's privacy: The fundamental advantage of PbD lies in its name, *the protection of user privacy*. By integrating data protection into the development process from the outset, companies can ensure that personal data is handled securely and responsibly. This not only builds trust with users, but also ensures that the services and products provided meet the highest standards in terms of data protection. User anonymity and security thus become priorities, which has a positive impact on customer loyalty. Overall, Software must be built securely from the early stages of its life-cycle which will also improve businesses adaptation of the SDLC.[512]

ii. Strengthening the company's reputation: A company that implements privacy by design sends a clear message: 'Privacy is central to its values and business practices.' This proactive approach strengthens the company's reputation as a responsible player in the digital space.

iii. Reducing data breaches and liability risks: By integrating data protection measures from the outset, companies significantly reduce the risk of data protection breaches. This is crucial, as data breaches can not only have financial consequences, but also legal implications. In many ways, PbD has become the "holy grail" of data protection to the extent that it offers a governance strategy to prevent privacy and data protection problems before they happen, by seamlessly integrating the requirements of the law into system design.[513]

iv. Promoting innovation through trust: Trust is the foundation for successful innovation. Companies that implement privacy by design as an integral part of their business practices create an environment of trust for customers and partners. This trust enables companies to use data in more creative ways to develop innovative solutions. When customers feel that their data is protected, they are more willing to provide their data for new services or personalized offerings. Privacy by design thus promotes a culture of innovation based on trust.[514]

---

[511] Arzu Gürgen, "DATA PROTECTION: BY DESIGN AND DEFAULT." < https://www.researchgate.net/publication/389625338_DATA_PROTECTION_BY_DESIGN_AND_DEFAULT> 2025

[512] Umeugo, Wisdom, Kimberly Lowrey, and Shardul Pandya. 2023. "Factors Affecting the Adoption of Secure Software Practices in Small and Medium Enterprises That Build Software In-House." International Journal of Advanced Research in Computer Science 14 (2): 1–7. https://doi.org/10. 26483/ijarcs.v14i2.6955.

[513] Liane Colonna, "In Search of Data Protection's Holy Grail Applying Privacy by Design to LifeloggingTechnologies" in Ronald Leenes, Dara Hallinan, Serge Gutwirth and Paul De Hert (eds.) Data Protection and Privacy: Data Protection and Democracy (Hart Publishing 2019), 176.

[514] Privacy by design: protecting privacy and benefits for companies <https://www.eunetic.com/en/blog/privacy-by-design-benefits-and-challenges> 2023

8. Challenges of Integrating Privacy Principles into Systems, Services, AI Models and Digital Infrastructure.

i. Finances: One of the main challenges in implementing privacy by design is the financial burden. Integrating data protection measures from the outset often requires significant investment in technology, training and compliance measures.

ii. Technical complexity: Integrating data protection measures necessitates analysis of existing systems, identification of associated risks, and implementation of appropriate security controls. Conversely, hardware and software engineers struggle to innovate new security control designs that are resilient to new and emerging threats.[515]

iii. Resistance within the organization: Employees who are used to established processes may find change disruptive. Getting to a practical implementation of PbD and PbDf involves taking a people-centred approach. Both in terms of collaborating with the relevant people internally, as well as thinking about impacts on and risks to the individuals whose personal data you are doing things with.[516]

9. Conclusion and Recommendation

Privacy by design represents more than regulatory obligations, they are privacy necessities for the corporate world. Their integration minimizes data breaches, reduces litigation risks, and enhances consumer trust for companies. To overcome the challenges noted in this paper, it is critical to emphasize the long-term strategic benefits of privacy by design as an opportunity and not an obstacle. Organizations can view financial resources for privacy as an investment in their future, they can also manage complexities by training their staff on the principles of privacy by design and how to integrate them into their daily workflow. Ultimately, organizations should emphasize the benefits of privacy by design and involve employees in the implementation process especially given the increasing importance of privacy in the business world today.

[515] Slesinger, Ian, Lizzie Coles-Kemp, Niki Panteli, and Rene Rydhof Hansen. "Designing Through the Stack: The Case for a Participatory Digital Security by Design." 2023 In Proceedings of the 2022 New Security Paradigms Workshop, 45–59. NSPW '22. New York, NY: Association for Computing Machinery. https://doi.org/10.1145/3584318.3584322.
[516] Emma Butler, "Data protection by design and default – what does that mean really?" <https://dpnetwork.org.uk/data-protection-by-design-and-default-meaning/> 2024

Data Privacy and the Legal Practice: Ensuring Compliance in Nigeria's Emerging Tech Landscape

Opeyemi M. Ajakaye, Esq.
Cybarik Global Ltd.
Senior Cybersecurity Analyst
ajakayeo@gmail.com

ABSTRACT

Privacy, as both a legal and security concept, is fundamentally concerned with the protection of personal data. In recent years, it has become an increasing source of concern across professions, including the legal sector, due to the rapid adoption of emerging technologies. Tools such as cloud computing, artificial intelligence, and digital communication platforms are reshaping legal practice by enhancing efficiency, accessibility, and client–lawyer interactions. However, these same technologies simultaneously generate new vulnerabilities, including risks of data breaches, surveillance, data persistence, and challenges related to data sovereignty. The focus on legal practice is particularly critical because law firms routinely handle highly sensitive and confidential client information, making them attractive targets for data breaches. Despite this, legal practitioners are often perceived as lagging in the implementation of robust technical and organisational measures for data security and privacy compliance. This gap exposes both clients and legal practitioners to significant risks, undermining trust and professional responsibility. To address these challenges, law firms must adopt proactive strategies that balance technological innovation with privacy safeguards. Such strategies include structured privacy training for all staff, enforceable internal policies on data handling and digital tool usage, and stronger governance frameworks for the adoption of emerging technologies. By embedding privacy and security into the core of legal practice, firms can not only comply with regulatory requirements but also strengthen client confidence in an increasingly digital legal environment. This paper highlights the urgent need for Nigerian legal practitioners to anticipate and mitigate privacy risks, ensuring that professional ethics and data protection obligations remain central in a technology-driven era.

Keywords: Privacy Rights, Personal Data Protection, Nigeria Data Protection Act (NDP Act), Emerging Technologies, Legal Practice

1. Introduction

Digital technologies have profoundly reshaped legal practice, influencing how lawyers manage cases, conduct hearings, and communicate with clients. These innovations have introduced efficiencies in case management, virtual proceedings, and client engagement. However, they also pose significant challenges to the protection of personal data and the preservation of client confidentiality. In Nigeria, where the legal system is undergoing both technological modernisation and regulatory reform, the concept of privacy in legal practice has gained renewed urgency.

Privacy lies at the heart of the lawyer–client relationship. It is both a legal mandate and an ethical cornerstone, underpinning trust and professional integrity. Nigerian lawyers are bound by the Rules of Professional Conduct to uphold confidentiality, but the integration of emerging technologies has expanded privacy obligations beyond traditional boundaries[517]. The Nigeria Data Protection Act[518] marks a pivotal shift toward global data governance standards, imposing specific responsibilities on data controllers and processors—including law firms—to safeguard personal information, ensure data security, and uphold the rights of data subjects.

This paper explores the evolving meaning of privacy within Nigerian legal practice, particularly in light of emerging technologies. It contends that privacy in legal practice transcends regulatory compliance and constitutes a fundamental safeguard for client rights in a digital age. By examining privacy through the dual lenses of professional ethics and statutory obligations, the discussion illuminates the risks, responsibilities, and opportunities facing legal practitioners as they navigate the future of law in Nigeria.

2. Conceptual Foundation of Privacy in Legal Practice

The conceptual foundation of privacy in Nigerian legal practice is rooted in constitutional guarantees and common law principles, progressively expanded through modern data protection legislation. Traditionally understood as the "right to be let alone," privacy has evolved both globally and within Nigeria into a multifaceted legal right encompassing autonomy over personal data. Contemporary Nigerian legal thought, shaped by international developments and domestic reform, increasingly recognises privacy not merely as protection from intrusion but as a dynamic entitlement to control the collection, use, and dissemination of personal information.[519]

3. Key Foundations of Privacy

A comprehensive understanding of privacy in Nigerian legal practice begins with its constitutional recognition as a fundamental right and extends through statutory developments that have progressively codified and expanded its scope in response to technological and societal change. These key foundations will be explored in this section.

---

[517] Abdulrauf, L.A. and Fombad, C.M. 2017. "Personal data protection in Nigeria: Reflections on opportunities, options and challenges to legal reforms." *Liverpool Law Review*, 38, pp.105-134.
[518] The Nigeria Data Protection Act 2023 (NDP Act)
[519] Erugoh Desiree, 2023. "Right to Privacy and Data Protection in Nigeria: What Companies Should Know." *Modaq*, September 25. https://www.mondaq.com/nigeria/data-protection/1369394/right-to-privacy-and-data-protection-in-nigeria-what-companies-should-know

a) Constitutional Basis

Section 37 of the 1999 Constitution (as amended)[520] serves as the cornerstone of privacy rights in Nigeria. It guarantees the privacy of citizens, their homes, correspondence, telephone conversations, and telegraphic communications, thereby establishing a legal shield against unauthorised intrusion. By situating privacy within Chapter IV of the Constitution, the Nigerian legal framework affirms it as a fundamental human right. This classification empowers individuals to seek judicial enforcement in a High Court when their privacy is violated, reinforcing the right's justiciability and legal significance. The constitutional guarantee is grounded in the broader principle of safeguarding individual autonomy and dignity. Personal data protection is an attribute of privacy that the Constitution seeks to protect.[521] It protects citizens from unwarranted and unreasonable interference by both state authorities and private entities, reflecting a commitment to personal freedom and the rule of law.

b) Statutory & Regulatory Expansion

In response to the growing complexities of digital data governance, Nigeria has enacted a series of legislative instruments that expand the scope of privacy beyond constitutional guarantees. These statutes establish comprehensive frameworks for data protection, cybersecurity, and the responsible use of personal information in both public and private sectors.

c) Nigeria Data Protection Act (NDP Act, 2023)

The NDP Act[522] is the principal legislation governing data privacy in Nigeria. It modernises the legal framework by codifying global standards, drawing influence from international instruments such as the European Union's General Data Protection Regulation (GDPR)[523] The Act grants individuals a broad range of rights, including the right to be informed about how their personal data is processed, the right to withdraw consent, and the right to request correction or deletion of inaccurate information.[524] The Act further imposes legal duties on data controllers— entities that collect and determine the purpose of data processing such as a Legal Practice—to ensure that personal data is handled lawfully, fairly, and transparently[525]. Controllers are also required to implement appropriate security measures to prevent unauthorised access, breaches, or misuse and assist Data Processors in the fulfilment of their obligations[526].

d) General Application and Implementation Directive (GAID) 2025[527]

The GAID serves as a regulatory companion to the NDP Act, providing detailed guidelines for its implementation. It addresses critical issues such as the scope and applicability of the NDP Act[528],

---

[520]Constitution of the Federal Republic of Nigeria, 1999
[521] Erugoh Desiree, 2023. "Right to Privacy and Data Protection in Nigeria: What Companies Should Know." *Modaq*, September 25. https://www.mondaq.com/nigeria/data-protection/1369394/right-to-privacy-and-data-protection-in-nigeria-what-companies-should-know
[522] The Nigeria Data Protection Act 2023 (NDP Act)
[523] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016
[524] Section 34, Nigeria Data Protection Act 2023 (NDP Act)
[525] Section 29, Nigeria Data Protection Act 2023 (NDP Act)
[526] Section 29 (1), Nigeria Data Protection Act 2023 (NDP Act)
[527] Nigeria Data Protection Act General Application and Implementation Directive, 2025
[528] Article 1

lawful bases for data processing[529], cross-border data transfers[530], breach notification procedures[531], and mechanisms for the enforcement of data subject rights.

e) Cybercrimes (Prohibition, Prevention, Etc.) Act 2015

The Cybercrimes Act establishes a legal and regulatory framework for combating cyber-related offenses in Nigeria. It criminalises unauthorised access to electronic communications and mandates data retention and protection obligations for financial institutions and other entities. The Act plays a complementary role in safeguarding digital privacy by deterring cyber threats and promoting accountability in electronic transactions.

f) The Rules of Professional Conduct for Legal Practitioners, 2023

All communications, whether oral or written between a legal practitioner and a client made in the course of professional engagement are protected by legal professional privilege. This privilege imposes a duty on the lawyer to refrain from disclosing confidential information, exploiting such information to the client's detriment, or using it for personal gain or the benefit of third parties.[532] While the duty of confidentiality is fundamental to legal practice, it is not absolute. Disclosure may be permitted where the client consents after full disclosure, where required by law, professional conduct rules, or court order, and where necessary to recover legal fees or defend against allegations of misconduct[533]. Additionally, if a client intends to commit a crime, a lawyer may disclose information strictly necessary to prevent the unlawful act. These exceptions are narrowly construed to preserve the integrity of the lawyer–client relationship and to uphold the broader principles of privacy, justice, and professional ethics.

As established in the preceding discussion, privacy is constitutionally guaranteed in Nigeria and further reinforced through statutory enactments. Within legal practice, the protection of privacy and personal data is not only a constitutional obligation but also a professional ethical requirement[534] grounded in the principle of confidentiality. The implication of Nigeria Data Protection Act on legal practice also mandates the processing of personal information only under the grounds for legal basis[535] such as Consent, Contractual Obligation, Legal Obligation, Vital Interest, Public Interest and Legitimate Interest. Such processing must also be done under the principles of data processing[536] such as Fairness, lawfulness and transparency of data processing, Purpose limitation, Data minimisation and ethics, Storage limitation, Data accuracy, Data confidentiality, integrity and availability, Accountability, and Duty of care. These principles are not merely regulatory requirements but professional imperatives that reinforce trust in the lawyer–client relationship.

---

[529] Article 16
[530] Article 45
[531] Article 33
[532] Section 19 (1), Rules of Professional Conduct for Legal Practitioners, 2023
[533]Section 19(2), Rules of Professional Conduct for Legal Practitioners, 2023
[534] Rule 58 (1) & (2) Rules of Professional Conduct for Legal Practitioners, 2023; Adeife Olumo, 2023."A Review of the Rules of Professional Conduct (RPC), 2023." *Modaq*, August 7. https://www.mondaq.com/nigeria/money-laundering/1351588/a-review-of-the-rules-of-professional-conduct-rpc-2023
[535] Article 16 (2), Nigeria Data Protection Act General Application and Implementation Directive, 2025; Section 25, Nigeria Data Protection Act 2023 (NDP Act)
[536] Article 15, Nigeria Data Protection Act General Application and Implementation Directive, 2025; Section 24, Nigeria Data Protection Act 2023 (NDP Act)

4. Data Protection Principles in Legal Practice

Like any data controller or processor, the Nigeria Data Protection Act (NDP Act) requires legal practices to process personal data in accordance with established principles of data protection. The principles include:

1. **Fairness, Lawfulness, and Transparency:** Clients' personal data must be processed fairly, lawfully, and transparently[537]. This ensures that individuals are fully informed about how their data is collected, used, and shared, thereby reinforcing trust in the legal profession.
2. **Purpose Limitation**: Personal data should only be collected for specified, explicit, and legitimate purposes.[538] Legal practitioners must avoid repurposing client data in ways that are incompatible with the original intent, thereby safeguarding against misuse.
3. **Data Minimisation and Ethics:** Only data that is adequate, relevant, and limited[539] to what is necessary for the provision of legal services should be collected. This principle underscores the ethical duty of lawyers to respect client privacy by avoiding excessive or intrusive data collection.
4. **Storage Limitation**: Personal data should not be retained longer than necessary[540]. Legal practices must establish retention schedules that balance regulatory requirements with the obligation to delete or anonymise data once it is no longer needed.
5. **Data Accuracy**: Legal practitioners are obligated to ensure that client data is accurate and up to date.[541] Inaccurate records not only undermine legal representation but also expose firms to liability under the NDP Act.
6. **Confidentiality, Integrity, and Availability**: Firms must implement both technical and organisational measures to protect data from unauthorised access, alteration, or loss[542]. This principle reflects the dual responsibility of safeguarding confidentiality while ensuring data remains accessible for legitimate legal purposes.
7. **Accountability**: Legal practices must be able to demonstrate compliance with data protection obligations. This requires documentation, regular audits, and the adoption of governance frameworks that evidence a culture of accountability.[543]
8. **Duty of Care:** In addition to statutory compliance[544], lawyers owe clients a professional duty of care in handling personal data. This extends to anticipating risks, adopting

---

[537] Section 24 (1) (a) Nigeria Data Protection Act 2023 (NDP Act); Article 15 (1) (a) & Schedule 1, Nigeria Data Protection Act General Application and Implementation Directive, 2025
[538] Section 24 (1) (b) Nigeria Data Protection Act 2023 (NDP Act); Article 15 (1) (b) & Schedule 1, Nigeria Data Protection Act General Application and Implementation Directive, 2025
[539] Section 24 (1) (c) Nigeria Data Protection Act 2023 (NDP Act); Article 15 (1) (c) & Schedule 1, Nigeria Data Protection Act General Application and Implementation Directive, 2025
[540] Section 24 (1) (d) Nigeria Data Protection Act 2023 (NDP Act); Article 15 (1) (d) & Schedule 1, Nigeria Data Protection Act General Application and Implementation Directive, 2025
[541] Section 24 (1) (e) Nigeria Data Protection Act 2023 (NDP Act); Article 15 (1) (e) & Schedule 1, Nigeria Data Protection Act General Application and Implementation Directive, 2025
[542] Section 24 (1) (f) & (2) Nigeria Data Protection Act 2023 (NDP Act); Article 15 (1) (f) & Schedule 1, Nigeria Data Protection Act General Application and Implementation Directive, 2025
[543] Section 24 (3) Nigeria Data Protection Act 2023 (NDP Act); Article 15 (1) (g) & Schedule 1, Nigeria Data Protection Act General Application and Implementation Directive, 2025
[544] Section 24 (3) Nigeria Data Protection Act 2023 (NDP Act); Article 15 (1) (h) & Schedule 1, Nigeria Data Protection Act General Application and Implementation Directive, 2025

preventive measures, and ensuring that privacy protection is embedded in all aspects of legal service delivery. As the legal profession increasingly integrates digital tools and platforms, the application of these principles becomes more complex and demanding. **The following section examines emerging technologies and their implications for privacy within legal practice, highlighting the challenges and responsibilities they introduce for legal practitioners.**

Emerging Technologies and Their Impact on Legal Practice

Emerging technologies are reshaping legal practice in Nigeria by enhancing operational efficiency, broadening access to justice, and introducing novel areas of legal engagement.

The impact of emerging technologies includes:

i. **Artificial Intelligence (AI)**: Artificial intelligence (AI) is increasingly transforming legal practice in Nigeria by streamlining core functions and enhancing decision-making. Platforms such as LawPavilion, Lawpadi and Legalpedia automate legal research, enabling practitioners to access relevant case law and statutory materials more efficiently than traditional methods[545]. AI-driven predictive analytics allow lawyers to assess historical data and forecast case outcomes, thereby informing strategic legal advice. Additionally, AI-powered tools facilitate automated document review and contract drafting, reducing human error and significantly improving operational efficiency in routine legal tasks.

ii. **Cloud Computing** Cloud computing has become a transformative tool in modern legal practice, offering law firms scalable storage solutions, remote access to case files, and collaborative platforms for team-based work. By hosting client data and legal documents on secure cloud servers, firms can streamline workflows, reduce reliance on physical storage, and enable lawyers to work seamlessly across different locations.

iii. **Electronic Filing and Virtual Legal Practice:** Electronic filing and virtual legal practice have significantly reshaped the delivery of legal services in Nigeria. The adoption of electronic filing and court automation systems by several courts has enhanced procedural efficiency and broadened access to justice. In parallel, the rise of virtual law firms accelerated by the COVID-19 pandemic has enabled legal practitioners to offer remote consultations and services, thereby overcoming geographical limitations and improving access to legal support for clients across diverse regions.

iv. **Instant Messaging Platforms for Client Briefs:** The use of instant messaging platforms such as WhatsApp, Google Meet and Microsoft Teams has become increasingly common for obtaining client briefs and facilitating real-time communication. These platforms offer speed, convenience, and accessibility, allowing lawyers to gather essential case details quickly and maintain ongoing dialogue with clients[546]. For a growing number of clients particularly Nigerians in the diaspora, as well as individuals and small businesses, instant messaging platforms represent a more accessible and less formal medium of communication

[545] Law Pavillion, 2024. "LegalTech in Nigeria: What to Expect by 2025." *Law Pavillion*, September 12. https://lawpavilion.com/blog/legaltech-in-nigeria-what-to-expect-by-2025/
[546] Gallabox, 2025. "Enhance Legal Practice with WhatsApp for Lawyers", June 2. https://gallabox.com/blog/whatsapp-for-lawyers

than traditional email correspondence or in-person consultations. As legal practice continues to embrace digital transformation, it must also confront the growing privacy risks and challenges that accompany emerging technologies and data-driven systems.

The privacy risks arising from these emerging technologies and their application in legal practice are examined in the following section.

5. Privacy Risks in Technology-Driven Legal Practice

The advancements in technology give rise to critical privacy concerns, including heightened risks of data breaches, algorithmic bias, and the pressing demand for an updated legal and ethical framework capable of addressing the complexities of digital transformation. These risks will be discussed in this section.

i. **Data Breaches**: The increasing reliance on digital platforms for storing and managing sensitive client information exposes law firms to heightened risks of cyberattacks, unauthorised access, and data breaches[547]. Such incidents can compromise client confidentiality, damage professional reputation, and result in legal liability under data protection laws.

ii. **AI Data Persistence and Spillovers**: Artificial intelligence systems particularly machine learning[548] often process large volumes of personal data to perform tasks such as legal research, document review, and predictive analytics. These systems may inadvertently retain data beyond its intended retention period (known as data persistence), or collect information about individuals not directly involved in the legal matter (data spillover). Both scenarios pose significant threats to privacy and may contravene data minimisation principles.

iii. **Surveillance and Data Collection**: The deployment of AI-powered surveillance tools whether by law firms, corporate clients, or government agencies, raises ethical and legal concerns about mass data collection. These technologies can track biometric identifiers, geolocation, and online behavior, potentially infringing on individuals' rights to privacy and autonomy, especially when used without informed consent or adequate safeguards.

iv. **Data Sovereignty:** Data sovereignty poses a significant privacy risk in cloud computing because information stored on servers located outside a firm's home jurisdiction becomes subject to foreign laws and regulations[549]. For law firms, this means sensitive client data hosted abroad may be accessed by foreign governments, exposed to weaker privacy protections, or caught in conflicting legal frameworks. The lack of control over where and how data is stored undermines confidentiality obligations and increases the risk of non-compliance with local laws such as Nigeria's Data Protection Act (NDP Act).

---

[547] Nigeria Bar Association Section on Legal Practice (NBA-SLP), 2024. "Draft Privacy Guidance for Lawyers in Nigeria." *NBA*. https://nbaslp.org/wp-content/uploads/2024/04/Draft-Privacy-Guidance-for-Lawyers-in-Nigeria.pdf.
[548] Riya Chugh, 2023. "Data Privacy and the Legal Implications of Emerging Technologies." *JETIR*, November 23. JETIR2311433.pdf

Having examined the privacy risks associated with technology-driven legal practice, the discussion now shifts to strategies designed to strengthen compliance and safeguard client rights.

6. Strategies for Advancing Privacy Compliance and Safeguarding Client Rights

As legal practice becomes increasingly digitised, it is imperative for practitioners to adopt proactive strategies that uphold data protection standards and preserve client confidentiality. These measures are essential not only for regulatory compliance but also for maintaining professional integrity and public trust.

i. **Data Protection:** Legal practitioners must exercise caution when engaging with digital tools, particularly those powered by artificial intelligence. Sensitive client data and confidential information should never be input into AI systems. Where the use of such tools is unavoidable, all personal identifiers must be thoroughly redacted. Inputs should be limited to non-sensitive and publicly available information. Additionally, practitioners should opt out of data retention features and other optional settings that may lead to the storage or sharing of sensitive information, thereby minimising exposure to privacy risks.[550]

ii. **Privacy Compliance:** Legal practitioners in Nigeria are required to comply with applicable privacy laws and regulations, including the Nigeria Data Protection Act (NDP Act) and the General Application and Implementation Directive (GAID). Compliance entails ensuring that the collection, storage, and use of personal data are conducted in strict alignment with legal requirements[551]. This obligation extends not only to the protection of client information but also to the handling of data across multiple jurisdictions in which both the client and the lawyer may operate. By adhering to these standards, practitioners safeguard client privacy rights, uphold professional ethics, and mitigate the risks of legal liability.

iii. **Privacy Training and Awareness for Staff:** Privacy training is a critical component of compliance within legal practice. A Fishbowl survey from February 2023 found that 68% of employees using AI tools for work did not inform their bosses, a practice known as "shadow AI"[552]. Therefore, law firms must ensure that all staff members, from lawyers to administrative personnel, are regularly educated on their obligations under the Nigeria Data Protection Act (NDP Act), the General Application and Implementation Directive (GAID), and professional ethical rules. Training should emphasise the importance of confidentiality, secure handling of both physical and digital records, and the proper management of client communications. Staff should also be equipped to recognise and respond to potential data breaches or suspicious activity, with clear reporting channels in place. Ultimately, fostering a culture of privacy awareness reinforces professional integrity and strengthens client trust.

---

[550] Legal Practitioner's Liability Committee, 2023. "Limitations and risks of using AI in legal practice" https://lplc.com.au/resources/lplc-article/limitations-risks-ai-in-legal-practice

[551] Legal Practitioner's Liability Committee, 2023. "Limitations and risks of using AI in legal practice" https://lplc.com.au/resources/lplc-article/limitations-risks-ai-in-legal-practice

[552] Ryan Golden, 2023. "Most employees using ChatGPT, other AI tools for work aren't telling their bosses." *HR Drive*, February 7. https://www.hrdive.com/news/employees-using-chatgpt-ai-for-work-not-telling-bosses/642166/

iv. **AI Usage Policy for Staff:** Given the increasing reliance on artificial intelligence in legal practice, firms must establish clear policies governing its use. Staff should be prohibited from inputting sensitive or confidential client information into AI tools unless such data has been fully anonymised or redacted. Only vetted and approved AI platforms that comply with NDP Act standards should be used, and staff must be trained to critically evaluate AI outputs to avoid overreliance or the perpetuation of algorithmic bias. Documentation of AI usage should be maintained to ensure transparency and accountability in legal processes. Such a policy will safeguard client confidentiality while allowing firms to responsibly harness the benefits of AI.

v. **Implementing a Privacy Policy for the Legal Practice:** A comprehensive privacy policy is essential for ensuring compliance and protecting client rights within legal practice. This policy should align with the NDP Act, GAID, and international best practices, such as those reflected in the GDPR, and must clearly define procedures for data collection, storage, access, retention, and secure disposal. Clients should be informed about how their personal data will be processed, including their rights to access, correction, and deletion[553]. Internally, strict access controls should be implemented to ensure that only authorised personnel can handle sensitive information. Regular audits and monitoring mechanisms are necessary to evaluate compliance and identify areas for improvement. Finally, the policy should include enforcement provisions, outlining disciplinary measures for staff who breach privacy or confidentiality obligations. By embedding these principles into daily operations, legal practices can strengthen compliance, protect client rights, and uphold professional ethics.

vi. **Data Localisation and Contractual Safeguards:** To ensure full privacy compliance, law firms should carefully evaluate and select cloud service providers, prioritise data localisation where feasible, and incorporate robust contractual safeguards that align with domestic data protection requirements.

Having outlined strategies for advancing compliance and safeguarding client rights, attention must now turn to the future trends that will redefine privacy in legal practice.

7. Future Trends of Privacy in Technology-Driven Legal Practice

As technology continues to reshape the legal profession, the issue of privacy is set to become even more complex and dynamic. The growing reliance on digital platforms, artificial intelligence, and cloud-based systems means that law firms will face new challenges in safeguarding sensitive information while meeting rising client expectations. These future trends will not only influence how law firms manage data but also redefine the ethical and professional responsibilities of lawyers in a technology-driven environment.

i. **Greater Exercise of Privacy Rights by Individual Clients:** Beyond corporate clients, individual clients are becoming more aware of their privacy rights under laws such as the NDP Act. This trend will likely lead to increased demands for transparency, stronger consent mechanisms, and greater accountability from law firms in handling personal data.

---

[553] Part IV, Nigeria Data Protection Act General Application and Implementation Directive, 2025

ii. **Establishment of Dedicated Cybersecurity and Privacy Teams:** As privacy risks grow more complex, law firms will need to move beyond ad hoc measures and create specialised teams focused on cybersecurity and data protection. These teams will oversee compliance, conduct regular audits, and implement advanced security protocols to safeguard sensitive client information.

iii. **Rising Incidents of Data Breaches Targeting Law Firms:** Law firms are increasingly viewed as attractive targets for cybercriminals due to the volume of sensitive data they hold, and their often-weaker security compared to financial institutions. This trend suggests a future where breaches become more frequent, pushing firms to adopt stronger defenses and incident response strategies.

8. Conclusion

This paper has examined the constitutional foundations, statutory provisions, and professional ethical obligations governing privacy in Nigeria. It has been established that legal practitioners are bound both by law and by professional ethics to safeguard the personal data rights of clients in the course of providing legal services and executing client instructions. While emerging technologies have undoubtedly enhanced legal practice and improved communication with clients, they also introduce significant privacy risks, including data breaches, AI data persistence and spillovers, surveillance and data collection, and challenges of data sovereignty.

To mitigate these risks, several strategies have been proposed: exercising caution in the use of digital tools, ensuring strict compliance with applicable privacy laws and regulations such as the Nigeria Data Protection Act (NDP Act) and the General Application and Implementation Directive (GAID), promoting privacy awareness and training for all staff members, and implementing enforceable privacy and AI usage policies. Looking ahead, it is anticipated that clients will increasingly assert their privacy rights as awareness grows, compelling law firms to adopt stronger safeguards.

Furthermore, the future of legal practice will likely see the institutionalisation of dedicated privacy and cybersecurity departments within firms, reflecting the centrality of data protection to professional responsibility. However, the paper also foresees a rise in data breaches targeting law firms, given their status as repositories of sensitive information. This underscores the urgent need for proactive measures to ensure that privacy and cybersecurity remain at the core of legal practice in a technology-driven era.

Emerging Technologies and the Future of Data Protection in Nigeria: Safeguarding Rights in the Age of AI, Surveillance, and Digital Sovereignty

Sabo Sambo Ahmad
Bayero University, Kano, Nigeria
sabosambo081@gmail.com
&
Sani Rabiu Bello
Faculty of Law, Bayero University, Kano, Nigeria
srbello.pbl@buk.edu.ng

ABSTRACT

Technological innovation continues to reshape the global data protection landscape, introducing profound challenges to privacy, autonomy, and sovereignty. For Nigeria, the adoption of the Nigeria Data Protection Act (NDP Act) 2023 and the release of the General Application and Implementation Directive (GAID) 2025 represent ambitious steps toward aligning with international best practices while addressing risks posed by artificial intelligence, surveillance technologies, and cross-border data flows. This article critically examines three pressing domains: automated decision-making and profiling, facial recognition and video surveillance, and the evolving discourse on data sovereignty. Drawing on global precedents such as the Snowden revelations, the Cambridge Analytica scandal, and China's surveillance of Uyghur Muslims, the paper situates Nigeria's regulatory response within broader international debates. It highlights GAID's innovations, including mandatory Data Protection Impact Assessments (DPIAs), Interoperable Data Privacy Measures (IDPMs), and structured frameworks for cross-border transfers. Yet, enforcement challenges such as institutional weaknesses, low compliance rates, and limited public awareness remain. The analysis argues that meaningful compliance requires strengthening NDPC's technical capacity, institutionalizing audits, fostering public data literacy, ensuring accessible judicial remedies, and cultivating international cooperation. By bridging the gap between progressive legislation and practical enforcement, Nigeria can transform its nascent framework into an effective safeguard for data rights.

Keywords: Data Protection, Emerging Technologies, Artificial Intelligence, Surveillance, Cross-Border Data Transfer

1. Introduction

Everyday new technologies become integrated into our daily lives and with that, new challenges to the protection of personal data. The Nigerian Data Protection Act (NDP Act) has attempted to remain technology-neutral to ensure that the protection of personal data does not depend on the techniques used in processing and is adaptable to the use of new technologies. However, this is not as simple as it seems. For example, the Snowden revelations of 2013 caused many legal frameworks to crumble, necessitating a revolutionised approach to data protection laws.[554] Moreover, cybersecurity attacks, big data analytics, and the rapid pace at which technologies like Artificial Intelligence (AI), Blockchain, the Internet of Things (IoT), and Biometric Systems advance often present unique challenges that require additional regulation.[555] The potential is limitless, which necessitates data protection to evolve with the tides of emerging technologies.

This paper will consider three emerging issues in prominent domains: (1) automated decision-making, profiling, and artificial intelligence, (2) facial recognition technology and video processing, and (3) the newly emerged discussions on data sovereignty.

2. Automated Decision-Making, Profiling, and Artificial Intelligence

Data subjects are often unaware of the amount and type of information collected about them, as well as how this data can be connected and analysed using artificial intelligence (AI) technologies to infer sensitive personal characteristics.[556] For example, platforms like Amazon suggest clothes or products based on users' search histories, Google predicts sites and news likely to attract individual attention, and Netflix curates movies based on past watch lists. These everyday examples highlight the pervasive nature of AI-driven profiling in consumer experiences.

On a deeper level, research by Kosinski et al. revealed how combining seemingly innocuous data—such as Facebook "likes"—with limited additional information could predict a user's sexual orientation with 88% accuracy and ethnic origin with 95% accuracy.[557] The Cambridge Analytica scandal underscores the more troubling implications of such capabilities. In this case, data from over 87 million Facebook users was harvested without consent and analysed using a "five-factor model" of personality traits. This analysis provided insights into users' openness, benevolence, and other psychological tendencies, which were exploited to create personalised political ads designed to manipulate voter behaviour. These ads were tailored to target individuals' fears and biases, influencing their electoral decisions without their informed consent. Cambridge Analytica notably played a significant role in the 2016 U.S. presidential election, supporting Donald Trump's campaign, and participated in shaping elections globally.[558]

---

[554] In 2013, Edward Snowden revealed classified documents showing that the U.S. National Security Agency (NSA) conducted mass global surveillance, including bulk collection of phone records and internet communications. His leaks sparked worldwide debates on privacy, security, and government overreach.
[555] Elief Kiesow Cortez, ed., Data Protection Around the World: Privacy Laws in Action (Cham: Springer, 2020), 273.
[556] *Ibid* 274
[557] Michal Kosinski, David Stillwell, and Thore Graepel, "Private Traits and Attributes Are Predictable from Digital Records of Human Behaviour," Proceedings of the National Academy of Sciences 110, no. 15 (April 9, 2013): 5802, https://doi.org/10.1073/pnas.1218772110..
[558] Abhishek Vats and Claudia Masoni, "A Decade in Pixels: Analyzing Incidents of State-Sponsored Surveillance from the Last Decade," in Handbook on Research on Cyber Security, ed. Abhishek Vats (New Delhi: MAIMS and Guru Gobind Singh Indraprastha University, 2023), 231.

Automated decision-making refers to decisions made entirely through automated processes, without human involvement.[559] This concept is exemplified by platforms like Google, Amazon, and Netflix, where algorithms independently make predictions and decisions about user preferences.

Profiling, a more focused form of automated processing, involves using personal data to evaluate specific aspects of a person's life. These include predictions about their performance at work, economic situation, health, personal preferences, interests, behaviour, or movements.[560] The Kosinski study and the Cambridge Analytica case are prime examples of profiling, demonstrating how data can be weaponised to influence individual decisions on a grand scale.

Artificial intelligence compounds these risks as an advanced form of automated decision-making that facilitates profiling based on seemingly insignificant data points.[561] The integration of AI tools and methods creates significant threats to personal data, potentially undermining fundamental freedoms, including freedom of expression. As seen in the Cambridge Analytica scandal, profiling through platforms like Facebook can subvert democratic processes by manipulating electoral outcomes.

This concern is especially relevant in contexts like Nigeria, where public awareness of the risks associated with data use and AI technologies remains limited. With a largely uninformed population, the potential for misuse of these tools—such as targeted political manipulation—could have serious consequences for governance and democracy.

As AI and data analytics continue to evolve, their accuracy and ability to extract sensitive information will only improve, amplifying the need for robust legal and ethical safeguards. Without these protections, the unchecked use of automated decision-making and profiling poses grave threats to individual rights and societal integrity.

2.1.1 Post-GAID Reflection:

The release of the NDPC's General Application and Implementation Directive (GAID) 2025 has introduced new compliance obligations that directly respond to some of these concerns. Section 24 of the NDP Act, as clarified by GAID, requires Data Protection Officers (DPOs) to adopt Interoperable Data Privacy Measures (IDPMs)[562]. These measures are designed to align Nigerian practice with globally interoperable principles of data protection, encouraging controllers and processors to apply best practice templates that transcend jurisdictional limits.[563] Importantly, GAID also requires Data controllers or processors under these circumstances to carry out Data Protection Impact Assessment (DPIA) and to take into account disparate outcomes of data processing and Data Subjects' Vulnerability Indexes (DSVI) when deploying emerging technologies, including AI.[564]

---

[559] Nigeria Data Protection Act, 2023, sec. 65.
[560] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, art. 4(4).
[561] Elief Kiesow Cortez, ed., Data Protection Around the World: Privacy Laws in Action (Cham: Springer, 2020), 273.
[562] Nigeria Data Protection Commission, General Application and Implementation Directive (GAID), 2025, art. 35.
[563] NDPC, GAID, art. 35(7).
[564] NDPC, GAID, art. 43.

While these steps signal Nigeria's intention to move toward international best practices, their success will depend on the NDPC's enforcement capacity and organisations' ability to operationalise such sophisticated requirements. Without adequate resources, technical expertise, and awareness, IDPMs may risk becoming aspirational rather than practical. The challenge, therefore, is not only to legislate progressive principles but to ensure their effective implementation in Nigeria's unique institutional context.

2.2 Facial Recognition Technology and Video Processing

Nigeria is currently marked by a scarcity of surveillance cameras. While precise figures are unavailable, it is evident that surveillance systems are limited to select governmental buildings, private corporate premises, and a handful of private residences. However, with a growing middle-class population, rapid urbanization, infrastructure development, rising governmental needs, and increasing terrorist attacks, this landscape is poised to change dramatically.[565] The Nigerian surveillance camera market is projected to grow significantly, reaching a value of USD 241.5 million at a CAGR of 8.4% between 2025 and 2031.[566]

While this surge signals technological advancement, it also introduces practical challenges to data protection. Systematic monitoring of public and private spaces using audio-visual surveillance heightens the risk of infringing on individuals' privacy. Such technology makes it easier to identify and track individuals within monitored areas, creating a potent tool that, in the wrong hands, could cause significant harm. A chilling example of this is the Chinese government's treatment of Uyghur Muslims, which underscores the dangerous implications of unchecked surveillance.

In 2017, under the guise of countering terrorism, the Chinese government launched a mass data collection campaign targeting Muslim residents, particularly Uyghurs, in the Xinjiang region. Biometric data such as DNA samples, iris scans, and blood types were harvested from individuals aged 12 to 65 as part of the so-called "Strike Hard Campaign Against Violent Terrorism." Surveillance cameras equipped with sophisticated AI were installed across Uyghur communities, monitoring them 24/7.[567]

These systems utilised AI algorithms to predict behaviours or potential "extremist tendencies" based on arbitrary criteria such as having more than two children, using a backdoor instead of the front door, minimal social interactions, or engaging in Islamic practices like prayer or Quran reading. Alarmingly, these computationally racist predictions were used to justify imprisonments and other punitive actions. Meanwhile, the Han Chinese population—making up 35% of the region's total population—was exempt from such measures, exposing the campaign as a blatant exercise of state control and cultural suppression.[568]

In stark contrast, the European Union adopted a proactive approach to regulating surveillance and facial recognition technology, especially following the NSA leak. Beyond the General Data

---

[565] 6Wresearch, "Nigeria Video Surveillance Market" (Industry Report, 2025), https://www.6wresearch.com/industry-report/nigeria-video-surveillance-market.

[566] *Ibid*

[567] Abhishek Vats and Claudia Masoni, "A Decade in Pixels: Analyzing Incidents of State-Sponsored Surveillance from the Last Decade," in Handbook on Research on Cyber Security, ed. Abhishek Vats (New Delhi: MAIMS and Guru Gobind Singh Indraprastha University, 2023), 240.

[568] *Ibid* 241

Protection Regulation (GDPR), the European Data Protection Board (EDPB) issued specific guidelines for video surveillance and facial recognition systems. These guidelines emphasise that the purpose of monitoring must be clearly documented for each camera, and generic purposes such as "safety" are insufficient justification.[569]

For instance, if a shop owner in the EU wishes to install surveillance cameras, they must demonstrate a legitimate interest under GDPR Article 6(1)(f). This requires proving that vandalism is a documented and actual threat in the neighbourhood, not merely a general concern across the nation. Similarly, national laws requiring surveillance must align with GDPR principles to avoid violations.[570]

Unfortunately, Nigeria lags behind in this regard. Despite the Nigerian Data Protection Act (NDP Act) and its implementation framework, GAID, there are no specific provisions addressing video surveillance and facial recognition akin to the EDPB's comprehensive guidelines. The absence of such regulations creates a legal vacuum, leaving room for potential abuse.

2.2.1 Post-GAID Reflection:

The NDPC's GAID has also moved to fill a regulatory gap by mandating a Data Privacy Impact Assessment (DPIA) under Section 28 of the NDP Act whenever surveillance cameras are deployed in areas accessible to the public.[571] This provision reflects a clear borrowing from international practice, particularly GDPR Article 35, which requires DPIAs for high-risk processing operations such as systematic monitoring of publicly accessible spaces.[572]

This innovation is commendable because it embeds risk assessment, mitigation, and accountability into Nigeria's regulatory framework for surveillance technologies. However, the framework stops short of providing detailed criteria comparable to the European Data Protection Board's guidelines, which specify necessity, proportionality, and safeguards in concrete terms. Moreover, without strong monitoring and sanctioning mechanisms, organizations may treat the DPIA as a box-ticking exercise rather than a substantive safeguard of rights. Nigeria therefore faces the dual challenge of ensuring that DPIAs are not only conducted but meaningfully evaluated and enforced by the Commission.

2.3 The Newly Emerged Discussions on Data Sovereignty

The growing trend of collection and analysis of big data is automated, continuous, inexpensive, and opaque.[573] The National Security Agency leak (NSA leak) provides a chilling example of amassing such a meticulous data repository, across almost the entire world. The NSA also disrespected ideas of sovereignty and mined data extraterritorially against unaware foreign nationals, which included even politicians. The Five Eyes routinely exchanged the data obtained

---

[569] European Data Protection Board (EDPB), "Guidelines 3/2019 on Processing of Personal Data Through Video Devices" (2020), 9-10.
[570] *Ibid* 10
[571] NDP Act 2023, s. 28.
[572] GDPR, art. 35.
[573] Vats and Masoni, "A Decade in Pixels," 242.

by them, thus breaching the trust of their citizens by sharing personal data as a commodity. This raised fresh concerns about the idea of data sovereignty.[574]

Apart from the NSA leak, the world has, in recent times, witnessed a flagrant disregard of the concept of sovereignty. For example, triggered by the catalytic events of Russia's interference with the US general election and Brexit in 2016, these countries and regions became aware that their political systems were vulnerable to manipulation.[575] The recent COVID crisis constitutes the most recent catalytic event on data sovereignty, with countries worldwide relying heavily on global tech giants like Google, Apple, and Microsoft for contact tracing, vaccine distribution systems, and digital health passports.[576] This raised concerns about sovereignty over health data, as much of it was stored and processed in foreign jurisdictions, potentially exposing it to laws like the U.S. CLOUD Act.

Now, what do countries do on the verge of these political crises? They adopt policies shaped towards guarding their domestic data jealously.[577] For example, after the NSA leak, the EU adopted digital sovereignty with a focus on the economic aspect.[578] They made their laws extraterritorial in a bid to both protect their local data while at the same time bringing foreign entities and corporations within the ambit of their law. This gives the EU significant control over how data is processed within and outside its borders.

The US, on the other hand, adopts a colossal control and "splinternet" digital sovereignty by passing the US CLOUD Act. This Act allows government access to data stored by U.S. companies abroad. With its dominance in big tech (e.g., Apple, Google, Microsoft), the U.S. focuses on maintaining global leadership in digital governance and control.[579]

China was the pacesetter in the concept of digital sovereignty. Concerned about the overwhelming US hegemony,[580] the country has, as early as 2014, championed the idea of strict digital sovereignty. It adopted data localization policies and invested heavily in domestic alternatives to foreign technologies, such as Huawei for 5G and Baidu for search engines.[581] India followed a similar trend by adopting domestic tech capabilities and reducing reliance on foreign platforms.[582] To date, India has banned over 200 Chinese apps, citing national security concerns. Russia also adopts strict data localization, mandating that personal data of citizens be stored on servers within the country.[583]

Now, what do African countries do? Uninspired by the growing concerns about digital sovereignty, African countries are only waking up to the pressing issues of protecting individuals' data, and that

---

[574] *Ibid* 243
[575] Johannes Thumfart, "The Norm Development of Digital Sovereignty between China, Russia, the EU and the US," in Data Protection and Privacy: Enforcing Rights in a Changing World, ed. Dara Hallinan, Ronald Leenes, and Paul de Hert (Oxford: Hart Publishing, 2022), 1–45.
[576] *Ibid*., 12.
[577] *Ibid*., 5.
[578] *Ibid*., 1.
[579] *Ibid*., 25.
[580] Rogier Creemers, "China's Conception of Cyber Sovereignty," in Governing Cyberspace: Behaviour, Power, and Diplomacy, ed. Nazli Choucri, David Drezner, and Andrew Quigley (New York: Routledge, 2020), 107.
[581] Creemers, "China's Conception of Cyber Sovereignty," 110
[582] Thumfart, "Norm Development of Digital Sovereignty," 23.
[583] Times of India. "India Bans 200-Plus Chinese Mobile Apps in Boon for Paytm." February 8, 2023. https://timesofindia.indiatimes.com/gadgets-news/india-bans-200-plus-chinese-mobile-apps-in-boon-for-paytm/articleshow/97683653.cms.

too, in a less urgent manner. It remains to be seen how Nigeria and other African countries will grapple with the challenges posed by neglecting digital sovereignty, including undermining a nation's autonomy, security, and ability to thrive in the digital economy.

2.3.1 Post-GAID Reflection:

The issuance of the GAID has provided, for the first time, structured guidance on cross-border data transfers, a core component of digital sovereignty. Section 42 of the NDP Act, as operationalised by GAID, introduces three principal grounds for lawful transfer: (i) an adequacy decision by the Commission, (ii) a Cross-Border Data Transfer Instrument (CBDTI) approved by the Commission, and (iii) other lawful bases such as public interest, contractual necessity, or data subject consent.[584] The adequacy framework in particular reflects a deliberate attempt to mirror global best practice, requiring enforceable data subject rights, judicial redress, rule of law safeguards, and the existence of an independent supervisory authority in the recipient jurisdiction.[585]

The GAID also emphasises Data Sovereignty as an explicit objective of CBDTIs, marking a clear departure from the earlier NDP Regulation regime which made only generic references to international transfer. By setting conditions such as mutual legal assistance agreements, proportionality in public authority access, and recognition of international commitments, the Commission positions itself to exercise greater control over Nigeria's data flows.

Nonetheless, questions remain as to whether Nigeria currently has the institutional leverage to enforce these standards against larger digital powers or multinational corporations. Adequacy determinations require sustained technical expertise and international cooperation, which the NDPC must now cultivate. Moreover, the reliance on CBDTIs such as binding corporate rules and standard contractual clauses raises concerns about whether Nigerian regulators can effectively monitor compliance once data leaves its borders.

3. Compliance and Safeguarding Rights in Nigeria

Nigeria's implementastion of the NDP Act 2023 and the GAID 2025 reflects a bold step toward aligning domestic law with international best practice. Yet, the effectiveness of these frameworks depends on whether compliance mechanisms can function in practice. Regulatory enforcement by the NDPC paints an uplifting picture. In mid-2024 NDPC announced it had collected ₦400 million (about $266K) in fines from seven firms (four banks and three others) for privacy violations.[586] These penalties followed investigations into hundreds of breaches: by June 2024 NDPC had opened over 1,000 probes (notably some 400 involving digital lending apps).[587] In one high-profile case, Fidelity Bank was fined ₦555.8 million (approx. $353K) for unlawful processing

[584] Nigeria Data Protection Commission, General Application and Implementation Directive (GAID), 2025, Schedule 5 ("Guidance on Cross-Border Data Transfer").
[585] NDPC, GAID, Schedule 5(2).
[586] TechPoint report — "NDPC gets ₦400 million in fines from 7 companies for data breaches" (June 2024)
[587] Adedapo Adesanya, "Private Sector Data Compliance at 55%, Public Sector Yet to Reach 20% — NDPC," Business Post, June 12, 2024, https://businesspost.ng/general/private-sector-data-compliance-at-55-public-sector-yet-to-reach-20-ndpc/.

of customer data without consent.[588] Similarly, in July 2025 the NDPC imposed about ₦766 million on MultiChoice Nigeria for intruding on subscribers' privacy and illegal cross-border transfers.[589] In August 2025 the NDPC publicly ordered some 1,368 entities – predominantly banks, insurers, pension funds, brokers and gaming companies – to prove compliance within 21 days.[590]

These insights provide tangible evidence of the NDP Act's impact on regulatory enforcement, compliance and safeguarding Data subject's Rights, however more beckon to be called. For instance, Official figures in mid-2024 showed only about 55% of private-sector entities and a mere 15% of public institutions meeting their data obligations.[591] The NDPC itself acknowledges that recorded breach reports likely understate the true scale (noting many data subjects are unaware of their rights).[592] Compliance hurdles are compounded by institutional strains and legal uncertainty. For instance, initial guidance by the NDPC on "Data Controllers and Processors of major importance" entities and cross-border transfers was challenged in court, while a host of other organizations required clarification on their respective roles. In practice many companies lack dedicated DPOs or the resources to implement complex GAID requirements (DSVIs, CBDTIs, annual DPIAs, etc.), especially small businesses and public agencies. Broad public awareness of the NDP Act is still nascent, and NDPC is just building enforcement capacity (it has launched mass sensitization campaigns and certified hundreds of DPOs, but must scale up outreach).

Therefore, in a bid to make compliance more meaningful, it is essential to strengthen the capacity of the NDPC through adequate funding, technical training, and institutional independence in enforcement. Compliance should also be institutionalised by mandating Data Controllers and Processors to engage licensed Data Protection Compliance Organisations (DPCOs) for routine audits and Data Protection Impact Assessments (DPIAs), with the resulting Compliance Audit Returns duly filed with the Commission. Equally important is public education and data literacy, which would empower individuals to understand and assert their rights. Moreover, judicial and administrative mechanisms must guarantee quick, affordable, and impartial remedies for violations. Also, while the NDPC has taken commendable steps through partnerships with bodies such as the Office of the Privacy Commissioner of Canada, the Global Privacy Assembly, and the Cross-Border Privacy Rules Forum, more needs to be done in bridging this foundational steps and crystallizing them into binding adequacy decisions or other robust cross-border enforcement mechanisms.[593]

Finally, there's an urgent need to pre-empt solutions to algorithmic, biometric and facial recognition profiling in Nigeria. Early preventive steps needs to be taken where both regulatory

---

[588] "Nigerian Data Agency Fines Fidelity Bank for Breaches," Reuters, August 22, 2024.https://www.reuters.com/business/finance/nigerian-data-agency-fines-fidelity-bank-breaches-2024-08-22/.
[589] Nigeria Data Protection Commission, "Press Release: NDPC Fines Multichoice Nigeria N766,242,500 for Violating NDP Act," Facebook post (July 6, 2025).
[590] "NDPC Launches Probe into 1369 Nigerian Companies Over Data Privacy Violations," Nairametrics, August 25, 2025, https://nairametrics.com/2025/08/25/ndpc-launches-probe-into-1369-nigerian-companies-over-data-privacy-violations/.
[591] Adesanya, "Private Sector Data Compliance."
[592] *Ibid.*
[593] Office of the Privacy Commissioner of Canada, "Memorandum of Understanding between the OPC and the Nigeria Data Protection Commission," 2024, https://www.priv.gc.ca/en/about-the-opc/what-we-do/international-collaboration/memorandums-of-understanding/mou-nigeria/; "Nigeria Joins Global Cross-Border Privacy Rules (CBPR) Forum," AllAfrica, April 30, 2025, https://allafrica.com/stories/202505010063.html.

and technical safeguards are prioritised. The NDPC should issue clear and comprehensive guidelines on the ethical use of artificial intelligence (in decision-making), use of facial recognitions technologies and other emerging identity processing technologies and should require transparency, accountability, traceability, human oversight and explicit bans on use in contexts likely to infringe on fundamental rights.

4. Conclusion

Nigeria's adoption of the NDP Act 2023 and GAID 2025 marks a vital step toward addressing privacy risks posed by artificial intelligence, surveillance, and cross-border data flows. GAID's provisions, particularly mandatory DPIAs, Interoperable Data Privacy Measures, and structured transfer rules—signal alignment with global standards and a commitment to digital sovereignty. Yet, weak institutional capacity, low awareness, and box-ticking compliance threaten their impact. Strengthening NDPC, embedding robust audits, and promoting data literacy are essential to meaningful protection. With proactive enforcement and citizen engagement, Nigeria can bridge its implementation gap and emerge as a data governance leader in the Global South.

Predictive Analytics, AI, and the Future of Data Protection: Risks, Rights, and Regulatory Imperatives

Nathaniel Atansuyi, Ph.D[594] Oyelakun Temitope Ayanladun, Ph. D[595]
Mrs. Ogunkan Stella Kehinde[596]

ABSTRACT

Predictive analytics and Artificial Intelligence (AI) have become central to industrial decision-making across finance, health, marketing, and public services. Their twin promises are to improve efficiency and novel insights that also introduce acute data-protection risks: opaque automated decisions, large-scale profiling, group and individual harms, re-identification, and cross-border data flows. This paper blends contemporary academic literature with industry practice to analyse how predictive analytics challenges existing data-protection regimes and to propose pragmatic, operational compliance measures. Building on surveys of bias and fairness, privacy-preserving machine learning techniques (federated learning, differential privacy, secure multi-party computation), and guidance from regulators and standards bodies (NDP Act and GDPR interpretations, EDPB/ICO opinions, the EU AI Act, and NIST's AI RMF), the paper also develops a practical five-pillar compliance framework for organisations that deploy predictive models, contracts and skills (DPO/AI compliance roles, vendor management). The paper outlines a mixed-method approach; the integrative literature synthesis and practitioner heuristics, and it concludes with concrete recommendations for regulators and industry to align technical controls with human rights, including suggestions for standardising DPIA outputs for models, incentivising privacy-preserving R&D, and building regulatory sandboxes for high-risk predictive systems.

Keywords: Bias and Fairness, Data-Protection Risks, Federated Learning, Predictive Analytics, Privacy-Preserving Machine Learning

[594] Hallmark University, natansuyi@hallmarkuniversity.edu.ng;
[595] Ladoke Akintola University of Technology, taoyelakun@lautech.edu.ng;
[596] Ladoke Akintola University of Technology, skogunkan@lautech.edu.ng.

I. Introduction

Predictive analytics of both statistical and machine learning methods used to forecast behaviour, risk, or outcomes but in recent times, it has moved from niche analytics teams into mission-critical production systems across industries. Firms now routinely use AI models for credit scoring, claims prediction, hiring screening, clinical triage, and automated content moderation. These systems process large volumes of personal data, often fuse multiple datasets, and generate outputs that materially affect individuals and groups. That scale and impact make data protection central to trustworthy deployment: regulators and standards bodies worldwide are issuing guidance and rules to align AI practices with rights-preserving principles. Major instruments and frameworks now shaping practice include the Nigeria Data Protection Acts (NDP Act, 2023) and EU's General Data Protection Regulation (GDPR) as interpreted for AI, the European Union's AI Act (the first region-level AI regulation to follow a risk-based approach), and cross-sectoral risk management guidance such as the U.S. NIST AI Risk Management Framework (AI RMF).[597]

In this paper we asked; how should organisations that build and operate predictive systems translate legal and ethical imperatives into industry-grade practice that both mitigates risk and preserves innovation? We answer by synthesising recent literature and practitioner guidance to create a usable compliance blueprint focused on operational controls and measurement. The audience are practitioners (DPOs, data scientists, compliance officers, technologists) and scholars interested in the intersection of predictive analytics and data protection.

2. Literature Review

The intersection of predictive analytics, artificial intelligence (AI), and data protection has generated a rapidly expanding body of scholarship across computer science, law, and social sciences. Existing research highlights both the transformative potential of predictive systems in domains such as finance, healthcare, and security, and the parallel risks of bias, opacity, and regulatory non-compliance. A recurring theme is the tension between innovation and accountability: while advanced methods like federated learning and differential privacy promise stronger safeguards, they introduce new tradeoffs in accuracy, scalability, and oversight. Current literature converges on the need for risk-based governance, robust documentation, and enforceable regulatory frameworks to balance utility with rights protection as highlighted below:

i. Predictive Analytics: Industry Uses and Risk Vectors

Predictive models are embedded in lending, insurance underwriting, fraud detection, workforce automation, targeted advertising, and personalized health. In many contexts the outputs determine access to goods, services, or opportunities, which creates regulatory scrutiny when decisions result in adverse outcomes. Recent enforcement actions and regulator guidance highlight harms from inadequate DPIAs, opaque profiling, and poor vendor oversight. For example, several

[597] European Commission, "AI Act - Shaping Europe's Digital Future," European Commission, (overview of AI Act and risk-based approach). https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

national authorities have fined or admonished organisations for failing to meet data-protection standards when deploying large-scale analytics.[598]

ii. Fairness, Bias and Societal Impact

Studies have identified multiple sources of algorithmic bias. Data provenance issues arise when training data reflect historical inequalities or sampling imbalances. Label artifacts occur when ground-truth labels are noisy, incomplete, or themselves biased. Model architecture can amplify these problems through design choices such as feature selection or optimization criteria. Finally, deployment context that includes how and where a model is applied can create or worsen disparities. The literature stresses that addressing bias is not only a technical task. Achieving fairness requires context-specific metrics, inclusive stakeholder involvement in design and governance, and ongoing monitoring, rather than relying solely on algorithmic adjustments.[3]

iii. Privacy-Preserving Techniques and Tradeoffs

Privacy-preserving machine learning (PPML) including federated learning, differential privacy (DP), homomorphic encryption, and secure multi-party computation (SMPC) has matured into production patterns that reduce raw data centralization and leakage risk. This review examines these techniques' utility and limitations such as the DP providing formal leakage bounds that can reduce model utility depending on epsilon budgets; federated learning reduces raw data sharing but introduces heterogeneity, client privacy leakage, and operational complexity; cryptographic approaches ensure strong confidentiality at higher computational cost. This paper stresses careful threat modelling and measurement to pick the right technique for the use case.[599]

iv. Governance, Documentation and Auditability

Scholars and policymakers increasingly argue that transparency in AI and predictive analytics cannot be achieved without systematic documentation. Recommended tools include model cards, which summarise a model's intended use, performance, and limitations; datasheets for datasets, which describe dataset composition, collection methods, and known biases; and standardised Data Protection Impact Assessment (DPIA) outputs, which record risk evaluations and mitigation measures. These artifacts create an auditable trail that links technical design choices to accountability obligations. Regulatory frameworks such as the NIST AI Risk Management Framework (AI RMF), European Data Protection Board (EDPB) opinions, and ICO guidance explicitly require organisations to implement documentation, rigorous testing, and continuous monitoring to ensure compliance and foster trust.[600]

v. Regulatory Landscape and Risk-Based Approaches

The EU AI Act introduces a risk-based compliance regime (with stricter rules for "high-risk" AI systems), while NIST's AI RMF provides a voluntary, flexible approach emphasizing measurement, governance, and rights preservation. National authorities (EDPB, ICO) have published AI-related opinions clarifying how GDPR obligations (lawful basis, DPIAs, data minimization, rights to

---

[598] Reuters, "Fidelity Bank fined by Nigeria data protection agency over data breach" (example of enforcement action, 2024). https://www.reuters.com/business/finance/nigerian-data-agency-fines-fidelity-bank-breaches-2024-08-22/

[599] C. Zhang et al., "A Survey on Federated Learning," Elsevier, 2021 (survey of federated learning and applications). https://www.sciencedirect.com/science/article/abs/pii/S0950705121000381

[600] NIST, Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST Special Publication, 2023. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf

explanations) apply to model training and operation. These instruments converge on a risk-sensitive, evidence-based approach to governance.[1,4]

3. Methodology

This paper adopts a mixed integrative methodology designed to translate academic and regulatory insights into actionable practitioner guidance. First, we conduct a targeted literature synthesis across peer-reviewed databases, regulator publications, technical standards, and industry reports to capture state-of-the-art discussions on predictive analytics and data protection. Second, we apply practice mapping, drawing on operational tools such as DPIA templates, governance frameworks, and enforcement case studies to ground theory in real-world practice. Third, we develop a five-pillar operational framework aligning legal requirements with technical mitigations. While not based on new fieldwork, this methodology operationalizes recent scholarship and regulatory expectations into practical workflows.

i. **Integrative Literature Synthesis:** This study conducted targeted searches across peer-reviewed databases, regulator publications, technical standards (NIST, EDPB, ICO), and reputable industry reports to capture both technical and legal perspectives on predictive analytics and data protection. The review focused on four main areas: (i) surveys on algorithmic bias and fairness, (ii) literature on privacy-preserving machine learning (PPML), (iii) regulatory documents and guidance, and (iv) documented compliance practices and case studies illustrating operational challenges.[3,601]

ii. **Industry Heuristics and Practice Mapping:** Drawing on published guidance and documented industry practice (DPIA templates, model governance patterns, vendor management), we translate theory into practical controls. Where empirical case data is limited, we lean on regulator published enforcement examples and public guidance to infer practical gaps.

iii. **Framework Development:** We developed a five-pillar operational framework by iteratively mapping legal requirements to corresponding technical and organisational mitigations. The pillars include: (i) risk-tailored DPIAs, (ii) data governance and privacy-preserving machine learning (PPML), (iii) transparency and documentation, (iv) continuous monitoring, and (v) governance and skills development. To ensure the framework is both practical and compliance-oriented, it was validated against regulatory expectations, including the European Data Protection Board (EDPB), the UK Information Commissioner's Office (ICO), and the Nigeria Data Protection (NDP Act), as well as international standards guidance, particularly the NIST AI Risk Management Framework (AI RMF).[1]

iv. **Limitations:** This is not an empirical study based on original fieldwork; rather, it operationalises the recent literature and public guidance into practitioner workflows. Field validation with specific organisations is recommended as next work.

---

[601] Multiple surveys and reviews on bias mitigation and fairness in AI (2021–2024) - see Ferrara (2024) and MDPI/Applied reviews for operational guidance https://www.mdpi.com/2413-4155/6/1/3e.

3.1 Practical Framework: Five Pillars for Rights-Preserving Predictive Analytics

Below we describe each pillar, explain technical and organisational controls, and provide operational checklists that a practitioner can adopt.

3.1.1. Risk-tailored DPIAs for predictive pipelines

DPIAs are a legal instrument under GDPR for processing likely to result in high risk; regulators have explicitly flagged large-scale AI training and profiling as topics needing DPIAs. DPIAs must be adapted to predictive pipelines, incorporating model lifecycle risks (training, validation, deployment, update).[602] [603]

i. **Operational Controls & Checklist**
   a. Expand DPIA scope to include: datasets used for training (sources, linkage), model architecture and explainability limits, downstream decision processes, and third-party model/vend or dependencies.
   b. Quantify harms (financial, reputational, discriminatory, autonomy loss). Use scenario-based threat modelling to identify plausible misuse.
   c. Record lawful basis for processing and compatibility of secondary uses; document retention and deletion policies for model training artifacts (checkpoints, logs).
   d. Publish or make available an executive-summary DPIA for public accountability where possible; submit to supervisory authority when required.

ii. **Measurement & Evidence**
   a. Maintain a DPIA artifacts repository: risk register, mitigation decisions, test logs, and periodic review dates. Use versioning to track model evolution and re-assess risk at significant updates.

3.1.2. Data Governance, Minimisation, and Privacy-Preserving Modeling

The principles of data minimisation and purpose limitation remain central under GDPR and equivalent regimes; technical PPML techniques are tools to operationalise these principles. Surveys indicate federated learning and differential privacy reduce some risks but require careful operationalisation to avoid giving false assurances.[6]

i. **Operational Controls & Checklist**
   a. Implement data minimization procedures: Map data flows; avoid unnecessary identifiers; replace direct identifiers with pseudonyms before model training.
   b. Adopt PPML where feasible: for cross-entity collaborations, prioritize federated architectures with DP noise budgets; for centralized models, use DP during training and restrict access to gradients/checkpoints.
   c. Threat model for membership inference and model inversion attacks; perform adversarial tests and privacy-risk metrics (e.g., membership inference success rates).

---

[602] Emilio Ferrara, "Fairness and Bias in Artificial Intelligence: A Brief Survey of Sources, Impacts, and Mitigation Strategies," Sci. 6, no. 1 (2024). https://www.mdpi.com/2413-4155/6/1/3

[603] Multiple surveys and reviews on bias mitigation and fairness in AI (2021–2024) - see Ferrara (2024) and MDPI/Applied reviews for operational guidance https://www.mdpi.com/2413-4155/6/1/3e.

d. Record data provenance and consent metadata; enforce retention schedules and data deletion flows that include model artifacts derived from the data.

ii. Measurement & Evidence

a. Track DP epsilon values, evaluate tradeoffs between utility and privacy, log federated aggregation rounds and client participation for auditability.

3.1.3 Transparency, Documentation, and Subject Rights Facilitation

Transparency obligations under data-protection law translate into operational needs: explainable outputs, decision records, and accessible pathways for subjects to query and challenge automated decisions. Model cards and dataset datasheets operationalize transparency for technical teams and auditors. Recent regulator opinions stress clarity on training data use and lawful bases.[604]

i. Operational Controls & Checklist

a. Produce concise model cards for production systems: Purpose, intended use, training data summary, performance metrics (overall and subgroup), known limitations, and contact point (DPO).
b. Maintain decision logs: for each automated decision record input features snapshot, model version, score, decision rationale (if available), human overrides, and timestamp. These logs support rights-to-access, rectification, and contestability.
c. Implement a subject interface: accessible, plain-language notices about profiling and automated processing; clear opt-out or human review mechanisms for high-impact decisions.

ii. Measurement & Evidence

a. Audit completeness of model cards and decision logs during internal audits; measure latency from subject request to response to monitor compliance with statutory deadlines.

3.1.4 Continuous Monitoring: Fairness, Privacy Leakage, and Drift Management

Static pre-deployment checks are insufficient models degrade and social contexts shift. Continuous monitoring regimes provide early warning for performance decline, privacy leakage, or emergence of discriminatory patterns. The NIST AI RMF and industry guidance emphasize measurement and monitoring to operationalize risk management.[5]

i. Operational Controls & Checklist

a. Deploy monitoring pipelines that compute: Performance metrics (AUC, calibration), subgroup fairness metrics (e.g., disparate impact, equalized odds approximations), and privacy-leakage tests (membership inference probes).
b. Use concept-drift detection and trigger re-training or rollback policies when thresholds breach.

---

[604] Information Commissioner's Office (ICO), "Data Protection Impact Assessments (DPIAs)," ICO guidance and resources (UK GDPR). https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/

c. Correlate monitoring alerts with business KPIs and compliance thresholds; establish incident response playbooks for model-related harms (e.g., biased outcomes, privacy breaches).

ii. Measurement & Evidence

a. Define SLOs/SLIs for model fairness and privacy; log alerts, remediation actions, and time to remediate for audit trails.

3.1.5 Governance, Contracts, and Capability Building

Organisational structures must support technical controls. This includes appointing AI-aware Data Protection Officers, contracting standards for vendors (model providers, cloud), and cross-functional review boards that include legal, technical and domain experts. Regulatory guidance encourages demonstrable governance.[5]

i. Operational Controls & Checklist

a. Establish an AI governance committee including DPO, lead data scientist, legal counsel, and domain risk owners.
b. Standardize vendor contracts to include data protection clauses, logging and audit rights, model provenance warranties, and incident notification timelines.
c. Invest in capability building: privacy engineering, algorithmic auditing skills, and legal literacy for data scientists. Create playbooks for procurement, testing, and decommissioning.

ii. Measurement & Evidence

a. Track training completions for staff, vendor audit results, and minutes/actions of governance committee meetings.

4. Discussions: Integrating Legal Obligations and Technical Realities

These discussions bridge the gap between legal principles and technical implementation in predictive analytics and AI. While laws such as the NDP ACT and GDPR establish obligations around lawful basis, minimization, transparency, and rights, practitioners face challenges in operationalizing these requirements within data pipelines and machine learning systems. This section examines how legal duties can be mapped into engineering controls, explores the complexity of fairness and privacy measurement, assesses the tradeoffs of privacy-preserving techniques, highlights the alignment of standards with regulatory expectations, and underscores the role of organisational culture in sustaining compliance.

i. Law vs. Engineering: Mapping Obligations into Controls

NDP ACT, GDPR and similar laws specify principles (lawful basis, data minimization, purpose limitation, DPIAs, rights to access/rectification). Translating these into code and pipelines requires careful mapping: e.g., lawful basis for profiling must be documented and matched to DPIA results and subject notices; data minimization must be implemented via feature selection and PPML; subject rights require decision logs and human-review workflows. Regulatory documents (EDPB, ICO) increasingly provide AI-specific commentary that clarifies expectations about training data, legitimate interests and the need for contextual DPIAs. Practitioners should use these documents to validate DPIA scopes and mitigation adequacy.[8]

ii. Measurement Challenges and Metric Pluralism

Fairness and privacy metrics are not one-size-fits-all. Studies suggest that operational metrics must be chosen with stakeholder input, and multiple metrics should be monitored to capture different harm modes. Practically, organisations should maintain a metrics catalogue mapped to risk categories identified in the DPIA and include thresholds that trigger remediation.[6]

iii. Privacy-Preserving Methods: Realism about Tradeoffs

PPML techniques are promising but operationally complex. The literature cautions that federated learning still permits leakage via model updates; DP requires careful epsilon governance and can materially degrade model utility when strict privacy budgets are applied. The paper's practical recommendation is not to treat PPML as a panacea but as part of a layered approach, comprising data governance, access control, encrypted storage, and PPML combined reduce overall risk.[605]

iv. Standards and Regulatory Alignment: Benefit of Risk Frameworks

Frameworks like NIST AI RMF provide flexible mappings from risk to controls and align well with regulator expectations because they emphasize measurable outcomes and governance. The EU AI Act introduces binding obligations for high-risk systems that will affect many predictive use cases; organisations operating in or with EU subjects must treat the Act as a live compliance requirement.[5]

v. Organisational Culture and Incentives

Finally, this paper emphasizes culture: compliance must be embedded into product lifecycles. Incentives such as performance metrics for data scientists should include fairness and privacy KPIs, not only accuracy; procurement must weight privacy and auditability as first-class criteria.

5. Conclusions and Recommendations

Predictive analytics offers substantial benefits but also poses real privacy, fairness, and rights risks. Since 2020, the literature has matured to present both the harms and practical techniques to mitigate them. Regulators (EDPB, ICO, EU AI Act) and standards bodies (NIST) have converged on risk-based, rights-preserving approaches that require organisations to combine technical, organisational, and legal controls.

i. Key Recommendations:

This recommendation is actionable, industry-focused, and treats DPIAs as living documents for model lifecycles. Expand DPIAs to include model training/checkpoint artefacts and require re-assessment at meaningful model changes. (Operational: DPIA repository, versioned artifacts.)[7]

---

[605] European Data Protection Board (EDPB), Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, 17 Dec. 2024. https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf

a. Adopt Layered Privacy Controls: Combine PPML (where appropriate) with strict data governance, access controls, and encrypted storage that measure privacy through adversarial tests, DP epsilon tracking, and membership inference probes.[9]
b. Operationalize Transparency: Produce concise model cards and decision logs that enable subject rights and regulatory review; implement subject interfaces for contestability.[5]
c. Monitor Continuously: Instrument pipelines with drift, fairness, and privacy leakage metrics tied to SLOs; create remediation playbooks and track time-to-remediate.[5]
d. Invest in Governance and Skills: Create cross-functional AI governance committees, appoint AI-savvy DPOs, and require vendor contract clauses allowing audits and model provenance checks.[5]
e. Engage Regulators Proactively: Use regulatory sandboxes and seek clarifying guidance when deploying high-risk predictive systems, especially where national authorities have issued opinions on use of personal data in model training.[606]

ii. For Regulators & Standards Bodies

a. Standardise minimum DPIA outputs and model documentation templates to reduce compliance friction and increase comparability across organisations.
b. Encourage adoption of measurable privacy standards (e.g., guidance on acceptable epsilon ranges for sectoral uses) and support testbeds for PPML approaches.

iii. Future Research

a. Empirical studies of production PPML deployments to quantify practical utility/privacy tradeoffs.
b. Standardized benchmarks for fairness and leakage under real production drift scenarios.
c. Economic studies on the compliance costs and innovation tradeoffs introduced by region-level

[606] S. Z. El Mestari, "Preserving data privacy in machine learning systems," ScienceDirect (2024)-review on data protection risks in ML systems. https://www.sciencedirect.com/science/article/pii/S0167404823005151

Data Sovereignty in Africa: Balancing National Interests and Global Data Flows

Solomon Nwabueze
Privacy Hub Africa
info@privacyhubafrica.org

ABSTRACT

Over the last decade, a range of innovations have increasingly become pronounced – from the 5G internet connectivity to Artificial Intelligence (AI), Cloud computing, the Internet of Things (IoTs), blockchain, and the Metaverse. These emerging technologies have become a major strategic asset for Big Tech companies with a worldwide market that is expected to reach €2.2 trillion in 2025. Expectedly, they are heavily dependent on processing personal data, the new oil of the 4th industrial revolution (4IR). In Africa, many of the innovative technologies, startups, and big tech companies are run by foreigners who relegate Africa to the backseat while giving the continent little or no power to control personal data processed in its territory. Regardless, Africa must find a way to balance the flow of data that will drive innovation and still maintain control. This paper, therefore, seeks to provide a discursive assessment of how African actors are empowered concerning the data of their subjects. Through an analytical review, it is found that there is a lack of an adequate framework and proper data-related policies, particularly in terms of uniformity. The doctrinal research methodology has been adopted, and reliance is placed on journal papers, online resources, reports, and primary sources. It relies on "the conditional data transfer model" and also concludes by highlighting key lessons that can be drawn, such as the development of local data storage and processing capabilities, fostering international cooperation and agreements, and a robust framework, amongst others.

Keywords: Data Sovereignty, Emerging Technology, Data Localisation, National Interests, Global Data Flows.

1. Introduction

Recent statistics on connectivity and digital use in Africa indicate that the continent has the strongest annual growth worldwide, with a +5.2% exponential growth in mobile subscriptions and

+8.7% in internet users between 2018 and 2019.[607] Already, foreign investments in digital growth, which spans virtually all regions in Africa, also focus on financial loans and building infrastructure like backbone and end-mile cabling, among others.[608] Foreign Direct Investments (FDIs) have equally seen growth in cloud computing, AI solutions, and smart technology.[609] Consequently, any mobile application leaves digital traces collected by servers of big tech companies in Europe and in the United States of America (the USA), like Google, Apple, Facebook, X, and Telegram.[610]Needless to say, these Tech giants collect personal data and resell it at higher prices to companies, institutions, or third parties, which enables the buyers to understand the behaviour, the habits of their customers or even citizens to optimise their investments.[611] Ukwueze[612] adds that the collection and storage of an individual's personally identifiable information (PII) such as names, aliases, occupations, religious beliefs and affiliations, telephone numbers, bank account details, family information, biometric data, and so on have been the modus operandi of micro and small and medium enterprises (SMEs) like financial technology (Fintech) companies and Startups to survive and expand.[613]

In response, the African Union (AU) has prepared a Digital Transformation Strategy for Africa (DTSA) and recognised the need to step up collaborative efforts to advance the continent's digital economy.[614] This policy framework intends to promote digital transformation as a strategy for the socio-economic growth of African content and to highlight the strategic objective of establishing a digital single market in Africa by 2030, especially in light of the African Continental Free Trade Area (AfCFTA).[615] But in the end, it is highly theoretical. It is among the few governmental documents that address African data sovereignty. Ultimately. there is still nascent literature and scholarship on the practicality of the Agreement. To add more, the African Union Policy Framework on Data Protection has re-echoed that,[616] "Maximising the benefits of a data-driven economy and minimising the risks are highly dependent on enabling policy and regulatory frameworks that increase legitimacy and public trust in the management of data. Data infrastructure that enables an integrated data system is a key strategic asset for countries, but the

---

[607] Stefano Calzati, "'Data Sovereignty' or 'Data Colonialism'? Exploring the Chinese Involvement in Africa's ICTs: A Document Review on Kenya," *Journal of Contemporary African Studies* 40, no. 2 (2022): 270–85, https://doi.org/10.1080/02589001.2022.2027351 accessed 25 September 2025

[608] Stefano Calzati (*ibid*).

[609] İlka Gültekin, Khushi Jaiswal, and Unyime Enobong Eyo, *AI for AI: Using Artificial Intelligence to Accelerate Investment* (Graduate Institute of International and Development Studies, 2024), https://www.graduateinstitute.ch/sites/internet/files/2024-09/AI4AI_-Using-AI-to-Accelerate-Investments.docx---Khushi-Jaiswal.pdf accessed 25 September 2025

[610] Stefano Calzati (*ibid*).

[611] Yogesh K. Dwivedi et al., "Setting the Future of Digital and Social Media Marketing Research: Perspectives and Research Propositions," *International Journal of Information Management* 59 (2021): 102168, https://doi.org/10.1016/j.ijinfomgt.2020.102168

[612] Dike Justin Ibegbulem and Festus Okechukwu Ukwueze, "Deconstructing Nigeria's Data Protection Regime from Consumer Protection Perspective," *The Law, State and Telecommunications Review* 13, no. 1 (May 2021): 94–118, https://doi.org/10.26512/lstr.v13i1.31850.

[613] Chidebe Matthew Nwankwo and Collins Chikodili Ajibo, "Liberalizing Regional Trade Regimes Through AfCFTA: Challenges and Opportunities," *Journal of African Law* 64, no. 3 (October 2020): 297–318, https://doi.org/10.1017/S0021855320000194

[614] John Stuart, "How African Digital Economy Initiatives Are Shaping the Continent's Digital Future," *TralacBlog*, November 19, 2024, https://www.tralac.org/blog/article/16592-how-african-digital-economy-initiatives-are-shaping-the-continent-s-digital-future.html accessed 25 September 2025

[615] African Union, *The Digital Transformation Strategy for Africa (2020–2030)*, May 18, 2020, https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf

[616] African Union, *The AU Data Policy Framework*, July 28, 2022, https://au.int/sites/default/files/documents/42078-doc-AU-DATA-POLICY-FRAMEWORK-ENG1.pdf accessed 25 September 2025

scale, extent, and speed of change brought about by data-driven digital technologies make regulation complex and resource-intensive."[617]

Unlike Africa, to ensure that more data is available for use in the economy and society while maintaining sovereignty over data for businesses and individuals, the European data strategy has laid out a roadmap for the establishment of European data spaces.[618]Additionally, to become a global leader in responsible and trustworthy AI and to give European developers and manufacturers a competitive edge, the European Union has adopted a strategy for creating AI technologies that adhere to high ethical standards (i.e., consumers and users ultimately favour EU-compliant products).[619]

Although it must be appreciated that States are now coming up with and legislating on the subject of data protection, especially on this thorny issue, much is still left to be desired in Africa, especially when the issues are analysed closely. To put this paper in perspective, there is a dire need to conceptualise some terms that will be employed in this paper, going forward.

2. Conceptual Framework

a. Data Sovereignty:

Jean Bodin's sixteenth-century conception of 'sovereignty' highlights the rights of the State in its capacity as the ultimate decision-making body, with the ruler holding all the power.[620] When Jean-Jacques Rousseau promoted popular sovereignty above that of the ruling elite in the 18th century, the concept experienced a paradigm shift.[621] The notion of people's sovereignty, according to which the government serves as the representative of the people, propelled the development of modern democracy.[622] When narrowed down to the concept of data, it is interesting that eighty-nine (89) countries, including many African countries, supported the proposal, sponsored by Russia, Saudi Arabia, China, Sudan, and Algeria, for all governments to have equal rights to manage Internet numbering, naming, addressing, and identification resources.[623]Botswana, Burkina Faso, Burundi, Egypt, Gabon, Ghana, Kenya, Lesotho, Morocco, Mozambique, Niger, Nigeria, Rwanda, Senegal, South Africa, South Sudan, Sudan, Tanzania, Togo, and Zimbabwe were among the twenty-one (21) African countries that signed the proposal to acquire sovereignty over the development, administration, and control of all telecommunications services.[624]

The concept of "data sovereignty", therefore, describes the belief that information gathered or maintained in a specific geographic place, which includes financial data, intellectual property, or

---

[617] The African Union (*ibid*).
[618] Mark Flynn et al., *The Impact of 5G on the European Economy* (Accenture, February 2021), https://www.accenture.com/content/dam/accenture/final/a-com-migration/manual/r3/pdf/pdf-144/Accenture-5G-WP-EU-Feb26.pdf accessed 25 September 2025
[619] Mark Flynn and Others (ibid).
[620] Edward Andrew, "Jean Bodin on Sovereignty," *Republics of Letters* 2, no. 2 (2011): https://shc.stanford.edu/arcade/publications/rofl/issues/volume-2-issue-2/jean-bodin-sovereignty accessed 25 September 2025
[621] *Ibid.*
[622] *Ibid.*
[623] Tope Shola Akinyetun, "Digital Sovereignty in Africa: The Albatross of Digital Transformation and Autonomy," *Kujenga Amani*, May 19, 2023, https://kujenga-amani.ssrc.org/2023/05/19/digital-sovereignty-in-africa-the-albatross-of-digital-transformation-and-autonomy/ accessed 25 September 2025
[624] *Ibid.*

personal data, should be governed by local laws.[625]Data sovereignty regulations seek to guarantee that personal data is governed by the laws in effect in the countries where the users are citizens, whether they are entering credit card information into an e-commerce website or leaving comments on a social media platform.[626] Notably, certain models of data sovereignty aim to ensure that information created in one country remains physically located in that country. Others want to ensure that, even if data is processed or kept in another jurisdiction, the legal safeguards afforded to data generated in that jurisdiction will still apply. There are also certain models to ensure that, regardless of whether it is also processed or kept abroad, data created in a jurisdiction is at the very least still accessible to law enforcement in that country.[627]

Be that as it may, where data sovereignty is the norm, data controllers must adhere to the many regulatory frameworks that apply to the personal data of their subjects as soon as their data is processed. It is safe to say that businesses that thrive with the internet and online infrastructure must map their data to ensure that the relevant data protection standards are observed.

b. **Digital Assets**:

According to Investopedia, "a digital asset is anything that has been produced and saved digitally, can be identified and found, and has value. With the integration of technological advancements into our personal and professional lives, digital assets have grown in popularity and value."[628] It has long been accepted that digital assets with ownership rights include data, pictures, videos, written content, and more.[629] The majority of digital goods, such as a business's brand, have a monetary or intangible worth. Some digital objects, like a family photo on your phone that was shot at a get-together, may only be significant to the originator or one individual. Others could have something to offer a far larger audience. But with the advent of blockchain technology and cryptocurrencies in 2009, digital assets were once more redefined. Through tokenisation on a blockchain, anything in digital form became something that could be utilised to generate value.[630]

c. **Data Localisation**:

This concept builds around the freedom of each State in the international sphere to protect her sovereignty and citizens' information that might flow to other States through technology – breaching national security in the long run. For Margaret Rouse, "it is the act of storing data on any device that is physically present within the borders of a specific country where the data was generated" he continued thus "free flow of digital data, especially data which could impact government operations or operations in a region, is restricted by some governments."[631] Hiscock captures it as "the practice of storing and processing data in the same country where it was collected from"[632] Darryl Richardson chooses to adopt Wikipedia's definition to mean "a practice

---

[625] Cloudflare, "What Is Data Sovereignty?" *Cloudflare Learning Center*, https://www.cloudflare.com/learning/privacy/what-is-data-sovereignty/ accessed 25 September 2025

[626] Cloudflare (ibid).

[627] Cloudflare (ibid).

[628] Investopedia: Digital Asset: Meaning, Types, and Importance (17 May 2024) <https://www.investopedia.com/terms/d/digital-asset-framework.asp> accessed 20 February 2025.

[629] Investopedia (*ibid*).

[630] Investopedia (*Ibid*).

[631] Margaret Rouse, *'What does digitisation mean?'* (2023), **cited in** Ekanem B E Eyo and Catherine O Elemi, 'Digitisation of Information Materials in Academic Libraries in Nigeria: A Case Study of University of Cross River State Library, Calabar, Cross River State' (2024) *European Academic Research* XI(11) 1277.

[632] Robb Hiscock, "Explainer: Data Localization and the Benefit to Your Business," *OneTrust Blog*, March 30, 2022, https://www.onetrust.com/blog/explainer-data-localization-and-the-benefit-to-your-business/

where the local legislation requires the data about a nation's citizens or residents to be collected, processed, and/or stored inside the country, often before being transferred internationally." In addition, such data is usually transferred only after meeting local privacy or data protection laws.[633]

d. **Data Privacy & Data Protection**:

The AU Data Policy Framework defines 'data protection' as that which regulates how data is used or processed and by whom, and it ensures citizens have rights over their data. It goes on to specify that "it is particularly important in ensuring digital dignity, as it can directly address the inherent power imbalance between 'data subjects' and the institutions or people who collected data." Suffice it to say that data protection encompasses all the efforts of a State which include policies, rules, regulations, or guidelines that are geared towards the protection of how the personal data of data subjects are obtained, used, recorded, organized, stored, altered, copied to a third party, and disseminated by the data controller or data processor within or outside that particular jurisdiction. It has some core principles like the data accountability, data minimization, data accuracy, storage limitation, data security, transparency and fairness in obtaining and processing personal data, lawful basis for processing the data, and minimization in the purpose(s) for obtaining that data.[634]

In this circumstance, a provision is usually made for how the data subject will seek redress when there is a breach of this right. The person whose personal data is subject to processing is the data subject while the person or organization that processes this personal information, who is regulated under the data protection regime is the data controller. When the information is processed on behalf of the data controller is the data processor according to the ECOWAS Data Protection Supplementary Act. A third party comes into existence here where the personal data is required to be transmitted to another person, corporate organization, or public company who did not personally obtain consent from the data subject. - in such cases, the data subject must be duly informed and must provide explicit consent prior to the disclosure or sharing of their data with any third party. According to a guide to the EU GDPR by the information communication officer (ICO),[635] where an entity qualifies as a data controller or data processor under the applicable legal framework, specific statutory obligations attach to that status, and liability will arise under the law where a breach can be traced to the failure to discharge those responsibilities.[636]

3. Legal Frameworks in Africa

In Africa, important legislation and policies have been passed and adopted including the African Union's Data Policy Framework (AU Data Policy), the Convention on Cyber Security and Personal Data Protection (The Malabo Convention), the Economic Community of West African

---

[633] Robb Hiscock (n 26).

[634] *Ibid.*

[635] Information Commissioner's Office, *Guide to the General Data Protection Regulation (GDPR)*, version 1.0, May 2018, https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf accessed 25 September 2025.

[636] Article 1 of the ECOWAS Data Protection Act has defined personal data as "any information relating to an identified individual or who may be directly or indirectly identifiable by reference to an identification number or to one or several elements related to their physical, physiological, genetic, psychological, cultural, social, or economic identity. It can even be anything from a name, address, photo, email address, bank details, posts on social networking websites, medical information, and other unique identifiers such as a media access control (MAC) address, Internet protocol (IP) address, International mobile equipment (IMEL) number, International mobile subscriber identity number, personally identifiable information to mention a few.

States (ECOWAS) Data Protection Act 2010, the Trans-Pacific Partnership Agreement and its protocol, the South African Development Community (SADC) Model Law on Electronic Transactions and Electronic Commerce, and the African Continental Free Trade Area (AfCFTA) adopted the AfCFTA Digital Trade Protocol (AfCFTA DTP). However, only the African Union Digital Transformation Strategy for Africa (2020-2030) and the AU Policy speak directly to data sovereignty.[637] The policy recommendation specifies that:

> By 2030 all our people should be digitally empowered and able to access safely and securely to at least (6 mb/s) all the time where ever they live in the continent at an affordable price of no more than (1cts usd per mb) through a smart device manufactured in the continent at the price of no more than (100 usd) to benefit from all basic e-services and content of which at least 30% is developed and hosted in Africa.

Some of its objectives are noteworthy:

i. To create a harmonised environment necessary to guarantee investment and financing by setting up a digital sovereignty fund in order to close the digital infrastructure gap and achieve an accessible, affordable and secure broadband, across demography, gender, and geography;[638]
ii. To harmonise policies, legislations and regulations and establish and improve digital networks and services with a view to strengthening intra-Africa trade, intra-investment and capital flows and the socio-economic integration of the continent, while maintaining a relational balance with other continents in the context of networked economies (Digital economy, collaborative economy);
iii. To support the Agenda 2063 flagship Pan-African "E" programme through providing policies and strategies that lead to transformative e-applications and services, thereby making the digital revolution the basis for service delivery and ultimately transform Africa into a Digital Society. Language barriers and time zones for e-learning and telepresence component of the Pan-African e-Network to be removed;
iv. To implement laws, policies and regulations required to stimulate and accelerate digital transformation for national, regional and continental development; and
v. To enable the coherence of existing and future digital policies and strategies at regional and national levels and mobilise effective cooperation between institutions;

In relation to data sovereignty, the framework, while mapping out these objectives, concedes that:

> …a very large part of the IT content consumed in Africa comes from outside and Data Centers are the digital infrastructure that will allow the development of a local digital industry. Therefore, Africa needs Data Center Infrastructure designed to host mission critical servers and computer systems, with fully redundant subsystems. The main benefit of this infrastructure localisation on the continent will be cost savings on

[637] The Strategy recognizes that "The Digital Transformation Strategy for Africa will build on the existing initiatives and frameworks such as the Policy and Regulatory Initiative for Digital Africa (PRIDA), the Programme for Infrastructure Development in Africa (PIDA), the African Continental Free Trade Area (AfCFTA), the African Union Financial Institutions (AUFIs, the Single African Air Transport Market (SAATM); and the Free Movement of Persons (FMP) to support the development of a Digital Single Market (DSM) for Africa, as part of the integration priorities of the African Union. The Smart Africa Initiative has set the creation of a Digital Single Market in Africa as its strategic vision."
[638] Emphasis supplied.

> international connectivity and the latency decrease that will deliver a better application performance. The second interest is respect for data sovereignty, even though Africa is at the moment less restrictive, soon it will be necessary to ensure localization of all personal data of Africa's citizens.

A good infrastructure is necessary for robust data sovereignty and localisation. Thus, "A global challenge is that the nature of data flows and digital infrastructure threatens domestic data sovereignty. To exert control of data to safeguard sovereignty requires both infrastructure and law, but also the technical capacity to do so in a manner that can build trust."[639]

It must be emphasized that certain jurisdictions implement a limited transfer strategy through data localization policies, wherein the controller, whose jurisdiction differs from that of the subject or consumer, may be obliged to handle and keep data locally before its cross-border transmission.[640] Data localization and data sovereignty laws have been argued to help achieve several policy objectives, such as protecting fundamental rights like the right to privacy, which in turn promotes inclusive growth and innovation at home, meeting regulatory requirements that guarantee access to data for supervisory purposes, and ensuring national security because data localization reduces the risks of unauthorized access and protects the sovereignty of the States to retain the information of its citizens.[641]

4. Challenges to Data Sovereignty in Africa

i. Limited Infrastructure and the Lack of Interest:

According to the World Bank Group, Africa boasts of a sizable and skilled tech-savvy workforce that can build on digital advancements to drive innovation and productivity – creating a dynamic ecosystem that enables businesses to scale up successfully.[642] Unfortunately, at both the regional and national levels, the availability and utilization of digital assets are closely associated with economic growth, innovation, job creation, and inclusion, at both the national and regional levels.[643] The region's digital infrastructure coverage, access, and quality still lag behind other regions, and while 84% of African residents lived in areas with 3G service and 63% had access to 4G mobile coverage, only 22% were using mobile internet services.[644] Similarly, the gap between coverage and usage is large for broadband, with 61% of sub-Saharan Africans living within broadband coverage but not using it. In 2021, approximately 470 million people in Sub-Saharan

---

[639] African Union (ibid).
[640] Franziska Sucker and Alexander Beyleveld, *Cross-border Data Flows in Africa: Policy Considerations for the AfCFTA Digital Trade Protocol*, October 30, 2022, https://ssrn.com/abstract=4278748 or https://doi.org/10.2139/ssrn.4278748 accessed 25 September 2025.
[641] World Bank Group, *Digital Transformation Drives Development in Africa*, January 18, 2024, https://www.worldbank.org/en/results/2024/01/18/digital-transformation-drives-development-in-afe-afw-africa#:~:text=The%20region's%20digital%20infrastructure%20coverage,were%20using%20mobile%20internet%20services, accessed 25 September 2025.
[642] *Ibid.*
[643] World Bank Group, *Digital Transformation Drives Development in Africa*, January 18, 2024, https://www.worldbank.org/en/results/2024/01/18/digital-transformation-drives-development-in-afe-afw-africa#:~:text=The%20region's%20digital%20infrastructure%20coverage,were%20using%20mobile%20internet%20services, accessed 25 September 2025.
[644] *Ibid.*

Africa lacked proof of identity, which prevented them from fully enjoying essential public and private services.[645]

What is more, due to the disparities in the economic development in African countries, poorer nations are finding it difficult to monitor and keep track of ontrollers and processors' activities in their jurisdiction. To worsen matters, the concerned agencies are usually underfunded and ill-equipped. Even, data-related policies are not given adequate attention at the national level. As such, data privacy is simply not a priority for the everyday person in some jurisdictions; Agyei-Bekoe's research found "low privacy concerns among [his sample of Ghanaians], which are influenced by the national culture, specifically collectivist cultural society.[646] A lack of culturally-centered policy development in the data privacy space in Africa has also contributed to apathy and ignorance about its importance.[647] In surveying Ghanaians on their concerns about privacy issues, scholar Eric Agyei-Bekoe found that his interviewees generally lacked "awareness and understanding of privacy and data protection issues.[648]

ii. Inadequate Framework:

Inadequate protection of personal data poses a significant risk – orchestrated by loopholes in the legal framework. For instance, while some of the local frameworks do not provide penalties and strong monitoring mechanisms, others provide insufficient monetary provisions. While commenting on the Angolan Data Protection Law, for instance, Bryant notes "…the maximum penalty that the law imposes for failure to comply is 150,000 USD, which, depending on how these penalties are allocated, could be insufficient to deter large-scale violations from big tech companies."[649]

In Ghana, there is the Data Protection Act 2018, which has an enforcement structure overseen by the Data Protection Commission (DPC), which has been saddled with the responsibility of protecting the privacy of personal data by regulating the processing of personal information, especially regarding the obtaining, holding, the use, or the disclosure of the same. It is also charged with prosecuting offences for the breach. In Nigeria, the Nigerian Data Protection Commission under Sections 6 and 7 of the Nigerian Data Protection Act 2023 has been vested with several powers and responsibilities which include the issuance of directives, and guidance and the imposing penalties thereof.[650] However, it failed to give any prosecutorial powers to this Commission, even with the fact that issues of data privacy require some level of expertise that is not fit for any law enforcement body in Nigeria.

iii. The Lack of Uniformity:

There is a lack of consistency across Africa concerning the methods that can be used to safeguard privacy against Big Tech companies. Bryant notes:

---

[645] *Ibid.*
[646] Dominic N. Dagbanja, "The Right to Privacy and Data Protection in Ghana," in *African Data Privacy Laws*, ed. Alex B. Makulilo (2016), 229–231, https://www.worldbank.org/en/results/2024/01/18/digital-transformation-drives-development-in-afe-afw-africa#:~:text=The%20region's%20digital%20infrastructure%20coverage,were%20using%20mobile%20internet%20services, accessed 25 September 2025.
[647] Alex B. Makulilo. "A Person Is a Person Through Other Persons – A Critical Analysis of Privacy in Africa." *Beijing Law Review* 7, no. 3 (2016): 149–165. http://dx.doi.org/10.4236/blr.2016.73020
[648] *Ibid.*
[649] Justin Bryant. "Africa in the Information Age: Challenges, Opportunities, and Strategies for Data Protection and Digital Rights." *Stanford Technology Law Review* 24, no. 2 (2021): 390.
[650] See Section 7(a-p) of the Nigerian Data Protection Act 2023 (NDP Act 2023).

> While country-level legislation on data protection is being enacted in Africa, it is important to remember that most African countries still do not have comprehensive legal frameworks for data protection, and those that do face considerable obstacles in enforcement. As major gaps exist in Africa's data privacy landscape, challenges will persist for years to come.[651]

While some jurisdictions have mandated that their Data Protection Commission take a more restrictive stance regarding cross-border data transfers, others have chosen a more liberal stance that even permits verification methods.[652] Notably, most of these discrepancies can be attributed to the various institutional inequalities and the reluctance of the respective governments to enact and carry out suitable policies. This tactic does have certain disadvantages, though. Laws governing data localization in nations like Nigeria and Kenya may affect foreigners in other jurisdictions who want to handle data gathered from their citizens. In contrast, some countries still use subsidiary legislation as supplementary measures since they do not have robust data protection legislation.[653]

5. Balancing National Interests and Global Data Flows

There are three modes in the data governance regime at the regional level: the open data transfer model, the conditional data transfer model, and the limited data transfer model.[654] Each presents its opportunities and pitfalls. Take the open data transfer model, for instance,[655] there is a minimal regulatory burden, which allows for the greatest flexibility in the movement of data, which is most suitable for digital services trade and data value creation. Unfortunately, there are risks of the proliferation of standards across firms and jurisdictions, without guaranteeing any minimum standard for personal data protection.[656]

The limited data transfer model is not any better because stringent regulatory approval for international data transfers may require explicit or implied data localization and mandatory storage which can stifle digital growth and data flows. Yet, it offers the strongest form of data security and control. In the meantime, it all goes to the focus and particularities of each jurisdiction. If a country is concerned with promoting growth and fostering a digital economy, relying on the limited data transfer approach would not be the best option. Nonetheless, Africa needs to take into cognizance its growing economy with a nascent market opportunity for FDI in digital assets. Ensuring that it maintains control over its data while ensuring digital drive requires that there should be a balance. This is where the conditional data transfer approach works. Certain suggestions will be made to drive the point home.

i. Developing local data storage and processing capabilities

---

[651] *Ibid.*
[652] Alliance Law Firm. "Cross-Border Data Transfer: Navigating Compliance Under the NDP Act 2023." October 11, 2023. https://inplp.com/latest-news/article/cross-border-data-transfer-navigating-compliance-under-the-nigerian-data-protection-act-2023/ accessed 25 September 2025.
[653] *Ibid.*
[654] The AU Data Framework 2020, p 42.
[655] Here, there is relatively low a priori mandatory approval requirements, and voluntary private sector industry standards inform the free movement of data (eg. USA, APEC).
[656] The AU Data Framework 2020, p 42.

Developing local data storage and processing capabilities requires that Africa must build the necessary infrastructure and the local human capital. In this vein, African countries would need to revisit some of their policies that allow local participation in companies that deal with digital assets and innovative technology.

ii. Fostering cooperation and agreements

Corporations and agreements are pivotal to maintaining control. For instance, Meta and Google want more users, and African countries want private investment in technology to meet developmental goals.[657] Nonetheless, Big Tech corporations are also the only organizations that possess the capital to invest in expensive infrastructure projects. In 2021 Liquid Intelligent Technologies, owned by telecoms giant Strive Masiyiwa's Cassava Technologies, partnered with Meta to build a 2000 km long fibre cable across the Democratic Republic of Congo (DRC).[658] In Nigeria, where Airtel Africa is the second-largest mobile provider, Free Basics started offering free access to 80 pre-selected websites to the 46% of Nigerians who owned a mobile phone at the time.[659] Therefore, by promoting cooperation and negotiations, both parties would ensure a win-win approach.

iii. Training and Adequate Funding of Data Protection Agencies in Africa.

Having enough resources to oversee and operate the Data Protection Agencies (DPAs) operations is another crucial factor in this case. While conceding that there are differences in the economic power of each African state, half of this issue might be resolved, though, if the money (or a portion of it) recovered or obtained from defaulters could be used to finance the DPAs in conjunction with government incentives. It is noteworthy that African and European states may work together to secure funding for this crucial issue.

iv. Provision of a Robust framework

To empower their DPAs, it is recommended that African laws on data protection have an effective compliance and enforcement system. This can be done by outlining their working structure, apparatus, and organs while ensuring that they have the authority to prosecute violators of the local Data Protection Act without undue interference with their duties. Their functions should be clearly defined, and there should be sufficient options or enforcement mechanisms available. States without a National/Domestic Data Protection Act are encouraged to establish national priorities and create their comprehensive data flow strategies and legislative frameworks in compliance with the AU Data Protection Framework.

6. Conclusion

This study has examined data sovereignty in Africa through a legal and doctrinal lens, focusing on how cross-border data flows, emerging technologies and weak regulatory structures shape current governance outcomes. It shows that although African states increasingly recognise data as a strategic resource, existing legal and institutional responses remain fragmented, uneven and largely

---

[657] Leo Komminoth. "Can Africa Achieve 'Digital Sovereignty' in an Era of Big Tech?" *African Business*, January 21, 2023. https://african.business/2023/07/technology-information/can-africa-achieve-digital-sovereignty-in-an-era-of-big-tech accessed 25 September 2025.
[658] Leo Komminoth (*Ibid*).
[659] Leo Komminoth (*Ibid*).

reactive. Continental and regional instruments signal policy intent, but their impact is limited by poor coordination, weak enforcement and wide disparities in national regulatory capacity.

The analysis further demonstrates that the debate is not about rejecting global data flows, but about securing lawful control over how data is generated, transferred and used. A balanced legal approach that conditions cross-border data transfers on clear safeguards offers a more realistic path than rigid localisation or unrestricted openness. Such an approach allows African states to protect national interests while still participating in the global digital economy.

Ultimately, the study highlights that Africa's data governance challenges stem less from the absence of ideas than from gaps in implementation, institutional strength and legal clarity. Addressing these gaps through enforceable legal frameworks, coordinated regulation and sustained capacity building is essential if data sovereignty is to move from policy ambition to practical reality.

Strengthening Proactive Data Protection through DPIAs and Risk-Based Approaches

Ayomide S. Salau
Data Privacy Associate
salauayomide@gmail.com

ABSTRACT
Emerging technologies such as AI, IoT, and cloud infrastructure have amplified the complexity of privacy risks. Regulatory frameworks like the NDP Act and GDPR mandate Data Protection Impact Assessments (DPIAs) as essential instruments for risk governance. DPIAs are not mere compliance checklists; they are operational risk management tools that must be embedded across processes, products, procedures, applications, and infrastructure. The risk-based approach shifts accountability from regulators to data controllers, requiring organisations to quantify and mitigate privacy risks before deployment. This paper explores the tri-stage DPIA model—design, default, and deployment—within global regulatory contexts, emphasizing structured methodologies, automation tools, and domain-specific strategies. It argues for lifecycle-integrated DPIAs as a policy imperative to ensure enforceable privacy by design, default, and deployment in rapidly evolving technological ecosystems.

Keywords: Data Protection Impact Assessment, Risk-Based Approach, Privacy by Design, Emerging Technologies, Regulatory Compliance

1. Introduction

With advancements in artificial intelligence, biometrics, IoT, and cloud infrastructure[660], data ecosystems have undergone significant transformation—accelerating the scale, speed, and sensitivity of personal data processing. Operating within decentralized architectures, these systems facilitate automated decision-making and continuous surveillance, thereby introducing new privacy risk vectors. The inherent complexity of these technologies necessitates the development of structured and forward-looking governance frameworks

[660] Oxford Digital Public Infrastructure Research Lab. https://www.csae.ox.ac.uk/oxford-digital-public-infrastructure-research-lab.

Regulatory frameworks have responded with mandates for Data Protection Impact Assessments (DPIAs). Under Article 28 of the NDP Act and Article 35 of the GDPR, DPIAs are compulsory for processing activities likely to result in high risk to individuals' rights and freedoms. Nigeria's NDP Act aligns with this principle, requiring controllers to assess and mitigate privacy risks before initiating sensitive data operations. Globally, jurisdictions in Asia-Pacific and the Americas are converging toward DPIA-like obligations, though enforcement varies.

DPIAs are not compliance checklists. They are strategic instruments for risk identification, mitigation, and documentation. A DPIA maps data flows, evaluates necessity and proportionality, assesses rights impacts, and prescribes safeguards. It enables organisations to embed privacy into system architecture, restrict data exposure by default, and validate controls before deployment. This tri-stage model—**design, default, and deployment,** aligns with the P4D3 framework.

The FAIR model (Factor Analysis of Information Risk) exemplifies this shift[661]. It quantifies risk by estimating threat frequency, susceptibility, and loss magnitude. Platforms like SAFE One automate FAIR assessments, integrating threat intelligence, control analytics, and loss modelling into continuous risk management. These tools convert DPIAs from static documents into dynamic, decision-support systems.

In the context of emerging technologies, DPIAs must be domain-specific, lifecycle-integrated, and enforceable[662]. They must apply across processes, products, procedures, applications, and infrastructure. Only then can DPIAs fulfill their regulatory and ethical function: safeguarding rights in environments where data is both an asset and a liability.

2. Policy Problem

Current privacy assessments in the context of emerging technologies are beset by fragmentation, reactivity, and a persistent misalignment with operational realities. Most organisations still approach Data Protection Impact Assessments (DPIAs) as box-ticking exercises, initiated only in response to regulatory audits or external scrutiny, rather than as proactive instruments for risk prevention. This reactive stance not only diminishes the preventive power of DPIAs but also increases the likelihood that data subjects will be exposed to unaddressed and evolving privacy risks[663].

A central shortcoming lies in the lack of domain-specific DPIA methodologies. While generic templates are widely used, they fail to accommodate the distinct threat profiles introduced by advanced systems such as AI-driven analytics, biometric authentication, mobile applications, internal monitoring platforms, and complex cloud infrastructures. Each of these domains presents unique risk vectors—including algorithmic bias, continuous surveillance, and cross-border data flows—that are not adequately captured by one-size-fits-all assessment models. Without tailored, context-aware methodologies, DPIAs are reduced to superficial checklists, incapable of identifying nuanced vulnerabilities or prescribing targeted safeguards[664].

---

[661] Cronk, R. Jason, and Stuart S. Shapiro. https://www.fairinstitute.org/blog/analyzing-privacy-risk-using-fair.
[662] Secure Controls Framework Council. https://securecontrolsframework.com/content/cdpas.pdf.
[663] El-Gazzar, Rania, and Karen Stendal. https://doi.org/10.5325/jinfopoli.10.2020.0237.
[664] Sion, Laurens, Dimitri Van Landuyt, and Wouter Joosen. "A DPIA Repository for Interdisciplinary Data Protection Research."

Moreover, privacy by design and default principles are rarely embedded into technology development lifecycles. Development teams, often pressured by market demands, prioritize rapid deployment and feature delivery, relegating privacy considerations to an afterthought. As a result, DPIAs are excluded from agile workflows, DevOps pipelines, and strategic product planning. This systemic disconnect produces systems that are inherently privacy-invasive, necessitating costly and inefficient retroactive fixes once issues are discovered[665].

The absence of structured DPIA execution across the tri-stage assessment model—design (privacy embedded in architecture), default (restrictive data flows and access), and deployment (real-world validation and stakeholder feedback)—further exacerbates compliance gaps and ethical risks. When risk assessments are conducted in silos, remain static, or are decoupled from ongoing system evolution, they quickly become obsolete. As emerging technologies scale and adapt, the initial DPIAs lose relevance, leaving organisations unaware of new or shifting threat landscapes.

Additionally, the slow adoption of automated assessment tools and structured frameworks undermines the efficacy of privacy governance. Platforms that operate methodologies like FAIR Privacy and CDPAS, or that automate DPIA processes (e.g., TrustArc, MineOS), have demonstrated their capacity to transform static assessments into dynamic, continuous decision-support systems[666]. However, these tools are not yet standard practice, and their absence perpetuates manual, inconsistent, and non-auditable DPIA processes.

Addressing these challenges demands urgent regulatory and methodological reform. Policymakers must mandate the integration of DPIAs throughout the entire system lifecycle—making them domain-specific, enforceable, and supported by automation. Regulatory guidance should require that privacy risk assessments are embedded at the design, default, and deployment stages, ensuring that controls are both preventive and adaptive. Only through such proactive, lifecycle-integrated governance can privacy assessments meet the demands of rapidly evolving domains like AI, biometrics, IoT, and cloud computing. Without this shift, privacy governance will remain reactive, fragmented, and inadequate for safeguarding individual rights in the face of technological advancement.

3. DPIAs Across Domains

Data processing in Nigeria and around the globe spans a wide array of operational domains, each presenting distinct privacy risks and regulatory challenges. As digital banking, biometric voter registration, and other emerging technologies proliferate, the pace of innovation has outstripped the implementation of structured, lifecycle-integrated privacy assessments[667]. To ensure meaningful protection of data subjects, Data Protection Impact Assessments (DPIAs) must evolve to be domain-specific, capturing the complex nuances of risk exposure and legal obligations unique to each environment.

---

[665] Wade, Jeff.. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2025/achieving-seamless-privacy-by-design-through-secure-by-design-practices.
[666] TrustArc. https://trustarc.com/products/privacy-data-governance/assessment-manager/. MineOS. "Automation-Driven Privacy, Security & Compliance." MineOS. https://www.mineos.ai/.
[667] "Wearable Tech in Nigeria: Privacy Risks and Regulatory Gaps.". https://businessday.ng.

a. Processes

Customer onboarding in Nigerian banks now routinely involves biometric capture, Bank Verification Number (BVN) validation, and real-time credit scoring, all of which introduce new vectors for privacy risk. Fraud detection systems rely on behavioural profiling and transaction monitoring, often leveraging advanced analytics and artificial intelligence. Data sharing workflows between financial institutions and fintech companies frequently lack granular consent mechanisms and transparency, increasing the risk of unauthorised profiling and third-party exposure. Effective DPIAs should not only assess risks related to profiling and data minimization failures but also examine the robustness of consent management, interoperability of systems, and the potential for algorithmic bias in decision-making. Additionally, as Nigerian banks expand digital onboarding to rural and underserved populations, DPIAs should consider the implications for digital literacy, informed consent, and equitable access to financial services.

b. Products

Smart electricity meters deployed by Nigerian distribution companies collect granular usage patterns and geolocation data, often transmitting this information to centralized servers for analysis and billing. Wearable devices used by health tech startups continuously monitor vital signs and relay sensitive health data to cloud infrastructures, sometimes spanning multiple jurisdictions. Fintech applications, such as mobile lending platforms, routinely access contact lists, SMS history, device metadata, and behavioural data, raising concerns about excessive data collection and opaque algorithmic decision-making[668]. Comprehensive DPIAs must address not only the risks of continuous data collection and algorithmic opacity, but also the adequacy of user controls, transparency of data processing, and resilience against unauthorised access or cyberattacks. Furthermore, as product ecosystems become more interconnected—such as wearables integrating with insurance platforms or smart meters linking with home automation systems, DPIAs should evaluate data sharing arrangements, interoperability standards, and user opt-out mechanisms.

c. Procedures

Human Resources departments in Nigerian firms manage sensitive employee data, including biometrics, health records, and disciplinary histories[669]. Surveillance policies in corporate offices extend beyond CCTV to encompass keystroke logging, email monitoring, and even remote desktop access[670]. DPIAs must rigorously evaluate access controls, transparency obligations, retention schedules, and audit mechanisms to prevent internal misuse, regulatory breaches, and employee privacy violations. In addition, DPIAs should address the ethical dimensions of workplace surveillance, balancing legitimate business interests with the rights of employees to privacy and dignity. As remote work becomes more prevalent, assessments should also cover remote monitoring tools, data transmission security, and cross-border employment scenarios.

---

[668] Federal Competition and Consumer Protection Commission (FCCPC). FCCPC.gov.ng, September 2025. https://fccpc.gov.ng/digital-lending-fccpc-tackles-abuses-issues-landmark-regulations/.
[669] Dentons ACAS-Law. https://www.dentonsacaslaw.com/en/insights/articles/2025/july/28/workplace-data-privacy-in-nigeria.
[670] DLA Piper Africa. https://www.dlapiperafrica.com/en/nigeria/insights/2025/workplace_surveillance_and_employee_rights.

d. Applications

- **Web**: Nigerian e-commerce platforms employ tracking pixels, third-party analytics, and behavioural advertising to personalize user experiences and optimize marketing strategies. DPIAs must scrutinize cookie policies, assess the risk of consent fatigue, and ensure compliance with evolving global standards such as the GDPR and Nigeria's NDPR. They should also evaluate the impact of data aggregation on user profiling and the risks associated with third-party data sharing.
- **Mobile**: Ride-hailing apps collect geolocation data, payment information, and device identifiers, often integrating Software Development Kits (SDKs) that transmit data to external servers, sometimes outside Nigeria. DPIAs should assess permission scopes, data flows, the security of data in transit, and the adequacy of user notifications regarding data usage. Special attention should be given to the risks of location tracking, profiling of movement patterns, and potential misuse by malicious actors.
- **Internal Tools**: Customer Relationship Management (CRM) systems in Nigerian banks monitor staff-client interactions, while employee productivity tools log activity and screen time. DPIAs must address surveillance boundaries, role-based access controls, and the potential for function creep, where tools designed for productivity monitoring expand into areas of personal surveillance. Regular reviews and updates to DPIAs are essential as internal tools evolve and new functionalities are added.

e. Infrastructure

Cloud platforms utilised by Nigerian startups and enterprises frequently host sensitive data in foreign jurisdictions, raising complex issues around cross-border data transfers, data sovereignty, and compliance with local and international regulations. Edge computing solutions in smart city initiatives process real-time traffic patterns and surveillance data, amplifying risks related to mass data collection and potential misuse by state or non-state actors. Data lakes in telecom companies aggregate vast amounts of subscriber information, creating attractive targets for cybercriminals and increasing the challenge of effective data governance[671]. DPIAs must thoroughly address risks associated with cross-border transfers, vendor lock-in, breach exposure, and the resilience of disaster recovery protocols. They should also consider the evolving threat landscape, including ransomware, supply chain attacks, and insider threats, ensuring that privacy safeguards adapt to new vulnerabilities as they arise.

Ultimately, the rapid deployment of emerging technologies in Nigeria demands a proactive, comprehensive, and context-aware approach to privacy governance. DPIAs must be continuously updated, embedded across the technology lifecycle, and supported by automated tools and structured frameworks.

Domain	Examples	Risks
Processes	Customer Onboarding, Fraud Detection	Profiling, Data Minimization failures
Products	Smart meters, wearables, fintech apps	Continuous data collection, opaque algorithms

[671] PwC Nigeria. https://www.pwc.com/ng/en/assets/pdf/cybersecurity-privacy-nigeria.pdf.

Procedures	HR data handling, surveillance policies	Excessive access, lack of transparency
Applications (Web)	E-commerce platforms, tracking pixels	Consent fatigue, hidden data flow
Application (Mobile)	Ride-hailing apps, SDKs, location tracking	Permission overreach, third-party data sharing
Application (Internal Tools)	CRM Systems, employee monitoring	Surveillance boundaries, role-based access
Infrastructure	Cloud platforms, edge computing	Cross-border transfers, vendor lock-in

4. DPIAs Across Lifecycle Stages

Privacy risks evolve throughout the lifecycle of a technology system. DPIAs must be conducted not as one-time exercises but as iterative assessments aligned with three critical stages: **design, default, and deployment**[672]**.** This tri-stage model ensures that privacy is embedded structurally, configured operationally, and validated contextually.

a. Privacy by Design

Privacy by design is a foundational principle that mandates integrating privacy considerations directly into the architecture, logic, and workflows of systems from the very beginning rather than treating them as afterthoughts. This proactive approach involves several structured activities:

- **Threat Modelling and Data Flow Mapping**: System architects should use established frameworks, such as LINDDUN, to systematically identify privacy threats, analyse data flows, and evaluate the ways personal data could be exposed, misused, or compromised. LINDDUN breaks down threats into categories—**Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, and Non-compliance**—making it easier to map risks to controls.[673]
- **Use of Privacy Engineering Tools**: Tools like Privado Scan and xCompass enhance the privacy-by-design process by automating the identification and contextualization of privacy risks. These tools map threat actors, mechanisms, and potential impacts, helping teams visualise vulnerabilities early in the development lifecycle and prioritize mitigation strategies.[674][675]
- **Enterprise Architecture Patterns**: Forward-thinking organisations are adopting enterprise architecture blueprints that embed the requirements of privacy laws, such as the Nigeria Data Protection Act (NDP Act), directly into core system design. This ensures that compliance is built-in from the start, reducing the risk and cost associated with retrofitting privacy measures after systems are already operational.

---

[672] Coface Group. "Appendix 06: Privacy by Design, Privacy by Default and DPIA Procedure." Coface.com.
[673] KU Leuven. "LINDDUN Privacy Threat Modelling Framework." LINDDUN.org,. https://linddun.org/.
[674] Privado Inc. "Open-Source Privacy Code Scanning." Privado. https://www.privado.ai/open-source.
[675] Comcast. "xCOMPASS (COMcast Privacy ASSistant)." GitHub. https://github.com/Comcast/xCompass.

By embedding privacy into both technical and organisational systems, privacy by design helps organisations not only meet regulatory obligations but also build user trust and resilience against emerging threats.

b. Privacy by Default

Privacy by default requires that systems, products, and services are configured to provide the highest privacy protection by default, without requiring any action from the user. This means collecting, processing, and exposing only the minimum data necessary for the intended purpose. Key mechanisms include:

- **Role-Based Access Controls (RBAC):** Implementing RBAC ensures that only authorised individuals can access specific data sets and functionalities, minimizing the risk of unauthorised exposure.
- **Anonymization and Pseudonymization Protocols**: Data should be anonymized or pseudonymized wherever feasible, reducing the risk of re-identification and limiting the impact of potential breaches.
- **Opt-In Configurations and Consent Management**: Features that require processing of sensitive or non-essential data should be deactivated by default and only enabled upon explicit user consent. The COFACE model, for instance, advocates for default settings that prioritize user privacy, deactivating data-intensive features unless users actively choose to enable them.
- **Privacy-Respecting Product Architectures**: Microsoft's privacy architecture for enterprise tools such as Copilot exemplifies best practices in enforcing data minimization and access boundaries through default configurations. These architectures are designed to limit data collection, restrict sharing, and provide transparent user controls.[676]

By ensuring privacy is the default setting, organisations demonstrate a strong commitment to protecting user data and complying with regulatory requirements such as the NDP Act and other global standards.

c. Privacy by Deployment

Privacy by deployment emphasises the importance of conducting a comprehensive DPIA immediately prior to launching or updating a system. This deployment-stage assessment validates that privacy controls are operationally effective in real-world scenarios. This process includes:

- **Testing for Unintended Data Flows**: Before deployment, systems must be rigorously tested to ensure that data is not being inadvertently exposed, leaked, or processed in ways not anticipated during the design phase.
- **Evaluating Mitigation Effectiveness**: All previously identified risks and implemented controls should be validated for effectiveness, with any residual risks documented and addressed.
- **Stakeholder Engagement and Feedback**: Gathering feedback from data subjects, business stakeholders, and operational teams helps identify real-world impacts and usability issues that may not have been evident during earlier phases.

[676] Microsoft. https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-privacy.

- **Automation and Auditability**: Platforms such as OneTrust automate deployment-stage DPIAs, integrating workflow management, stakeholder role assignment, and audit trails for regulatory compliance and future review.[677]

Deployment-stage DPIAs are especially critical for complex and dynamic systems like artificial intelligence and machine learning models, where operational behaviour can diverge from initial design assumptions. Continuous validation ensures that privacy protections remain robust as systems evolve.

Integrating DPIAs across the entire lifecycle—from design and default to deployment—transforms privacy governance from static documentation into a dynamic, adaptive risk management model. This approach not only aligns organisations with regulatory expectations under the NDP Act and other global standards, but also fosters a culture of accountability, responsiveness, and trust between organisations and their stakeholders.

5. Tools, Models, and Frameworks

Effective DPIA execution requires structured tools, quantifiable models, and automation platforms that support scalable, repeatable assessments. These instruments enable organisations to move beyond ad hoc compliance and embed privacy risk management into operational workflows.

DPIA Templates

Regulatory bodies provide standardised DPIA templates to guide assessments. The Nigeria Data Protection Commission's (NDPC) template includes screening checklists, risk evaluation matrices, and mitigation planning. UK's Information Commissioner's Office (ICO)[678] and France's CNIL offers sector-specific templates that assess proportionality, necessity, and data subject rights[679]. The NIST Privacy Framework provides a modular structure for integrating privacy risk into enterprise risk management.[680]

Risk Quantification Models

The FAIR Privacy model, developed by R. Jason Cronk and Stuart Shapiro, adapts the Factor Analysis of Information Risk (FAIR) methodology to privacy contexts[681]. It quantifies risk based on threat frequency, vulnerability, and impact severity, enabling comparative analysis across scenarios. The CDPAS framework, published by the Secure Controls Framework Council, standardizes privacy and cybersecurity assessments through defined control sets, maturity levels, and materiality thresholds[682].

---

[677] OneTrust. https://my.onetrust.com/s/topic/0TO1Q0000001olbWAA/pia-dpia-automation-deployment?language=en_US.
[678] Information Commissioner's Office (ICO). "Data Protection Impact Assessments." ICO.org.uk.
[679] Commission Nationale Informatique et Libertés (CNIL). "Privacy Impact Assessment (PIA)." CNIL.fr. https://www.cnil.fr/en/privacy-impact-assessment-pia.
[680] National Institute of Standards and Technology (NIST). NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0. Gaithersburg, MD: NIST, January 16, 2020.
[681] Cronk, R. Jason, and Stuart S. Shapiro. "Analysing Privacy Risk Using FAIR." FAIR Institute, April 5, 2022. https://www.fairinstitute.org/blog/analysing-privacy-risk-using-fair.
[682] Secure Controls Framework Council. https://securecontrolsframework.com/content/cdpas.pdf.

Automation Tools

Platforms like OneTrust and TrustArc automate DPIA workflows, enabling real-time risk flagging, stakeholder collaboration, and audit readiness. OneTrust's DPIA module integrates data mapping, threshold assessments, and escalation protocols for high-risk processing[683]. TrustArc offers customizable risk matrices, automated reporting, and regulatory guidance through its NymityAI engine[684].

These tools and frameworks operationalise DPIAs, transforming them from static documents into dynamic systems of accountability. They support lifecycle integration, cross-functional collaboration, and regulatory alignment—key requirements for privacy governance in emerging technologies.

6. Policy Recommendations

To ensure DPIAs evolve from regulatory checklists into strategic governance tools, the following policy interventions are necessary:

i. Mandate DPIAs for High-Risk Technologies Across All Domains

Regulators must enforce DPIAs for any processing involving AI, biometrics, IoT, cloud infrastructure, or automated decision-making. These technologies consistently meet the threshold for "likely to result in high risk" under Article 28 of the NDP Act. DPIAs should be compulsory across all domains—processes, products, procedures, applications, and infrastructure—where personal data is processed at scale or sensitivity.

ii. Develop Sector-Specific DPIA Guidance

Generic DPIA templates fail to capture domain-specific risks. Sectoral regulators should issue tailored DPIA frameworks for industries such as finance, health, education, and telecommunications. The European Data Protection Board's WP248 guidance and CNIL's sectoral DPIA templates offer scalable models[685]. These should be localised to reflect jurisdictional nuances, operational realities, and risk typologies.

iii. Incentivise Privacy Engineering and Cross-Functional Teams

Privacy engineering must be embedded into development lifecycles. Governments and regulators should incentivise organisations to build cross-functional privacy teams—comprising legal, engineering, product, and compliance units. Funding, certification programmes, and regulatory sandboxes can accelerate adoption. Privacy-by-design must be operationalised through tooling, not policy statements.

iv. Require DPIAs at Design, Default, and Deployment Stages

Lifecycle enforcement is critical. DPIAs must be conducted at:

- **Design**: Before architecture is finalized, using threat modelling and data flow analysis.

---

[683] OneTrust. "PIA & DPIA Automation Overview." MyOneTrust. https://my.onetrust.com/s/article/UUID-f5ba6a6d-2ac5-ea2b-5998-3d3bb9ada5e1?language=en_US.
[684] TrustArc. "A Practical Guide to DPIAs: Managing Risk, AI Ethics, and Global Privacy Regulations." TrustArc.com. https://trustarc.com/resource/guide-to-dpias-managing-risk-ai/
[685] https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/data-protection-impact-assessments-high-risk-processing_en.

- **Default**: During configuration, ensuring data minimization and access controls.
- **Deployment**: Prior to go-live, validating real-world risks and stakeholder impacts

This tri-stage model aligns with Article 28 of the NDP Act and emerging global standards. It ensures DPIAs are iterative, context-aware, and enforceable.

These recommendations reposition DPIAs as instruments of anticipatory governance, enabling organisations to manage privacy risks proactively and systematically.

7. Conclusion

Data Protection Impact Assessments (DPIAs) are no longer optional instruments of compliance—they are strategic mechanisms for anticipatory governance. As emerging technologies reshape data ecosystems, the risks to individual privacy intensify across domains and lifecycle stages[686]. Fragmented assessments, generic templates, and post-hoc evaluations are insufficient. DPIAs must be proactive, domain-sensitive, and embedded into the architecture of digital systems.

Regulators must enforce DPIA mandates for high-risk technologies and require assessments at design, default, and deployment stages. Sector-specific guidance must replace one-size-fits-all models. Developers must integrate privacy engineering into product lifecycles, and privacy officers must lead cross-functional teams that operationalise risk governance. DPIAs must evolve into dynamic, iterative processes that adapt to technological change and regulatory complexity.

This shift demands institutional commitment, regulatory clarity, and operational discipline. DPIAs must be treated not as compliance burdens but as instruments of trust, transparency, and accountability.

[686] PrivacyEngine.io. https://www.privacyengine.io/blog/a-guide-to-data-protection-impact-assessment-dpia/.

Balancing Innovation and Privacy: Advancing Data Protection and Governance in Nigeria's Digital Economy

Sunday Gideon Gumut
Abubakar Tafawa Balewa University, Bauchi
gideongumutgmail.com

ABSTRACT

Nigeria's digital economy is expanding rapidly, fueled by fintech, e-commerce, e-governance, and data-driven innovation. Yet this growth poses significant challenges around privacy, trust, inclusion, and security. This paper examines Nigeria's evolving data protection landscape within the context of the Nigeria Data Protection Act (NDP Act 2023), global regulatory trends, and African perspectives on digital rights. It explores the opportunities of a data-driven economy, the risks of surveillance and cybercrime, and the ethical dilemmas of balancing innovation with fundamental rights. Drawing on comparative insights from the EU, US, and China, the study argues that Nigeria must strengthen enforcement, embed ethics in innovation, and prioritise digital inclusion to ensure equitable growth. By combining strong regulation, corporate accountability, and citizen empowerment, Nigeria can position itself as a continental leader in rights-based digital governance. The findings offer actionable recommendations for policymakers, businesses, and civil society, making the case that a resilient digital future depends on safeguarding privacy as both a right and an enabler of innovation.

Keywords: Digital Economy, Data Protection, Privacy, Digital Inclusion and Cybersecurity

1. Introduction

Africa's digital economy is at a decisive threshold, one shaped by competing forces of innovation and vulnerability. The continent is witnessing rapid growth in internet penetration, mobile adoption, fintech services, and digital entrepreneurship. According to the World Bank, Africa's digital economy could contribute nearly $180 billion to GDP by 2025 if fully harnessed. [1] Yet, this growth is shadowed by systemic challenges—weak infrastructure, fragmented regulatory systems, and widening inequalities in access and skills. [687]

[687] World Bank, The Future of Africa's Digital Economy (Washington, DC: World Bank, 2021)

In Nigeria, the passage of the Nigeria Data Protection Act (NDP Act) in 2023 marks a significant step toward embedding data rights into the architecture of the country's digital economy. The law follows the earlier Nigeria Data Protection Regulation (NDPR) of 2019, which created the first structured compliance obligations for data controllers and processors. While the NDP Act aligns Nigeria with continental frameworks like the African Union's Malabo Convention and echoes elements of the European Union's General Data Protection Regulation (GDPR), it also raises deeper questions[688]: How can Africa safeguard fundamental rights while encouraging innovation? How can compliance be reframed from a legal burden into a catalyst for digital trust and competitiveness?

The answers to these questions are urgent. Emerging technologies, such as Artificial Intelligence (AI), Blockchain, the Internet of Things (IoT), and Biometric Surveillance, are expanding across Africa's public and private sectors. Nigerian fintech firms use AI-driven models for credit scoring, South African telecoms deploy biometric authentication, and Kenyan agriculture projects rely on IoT sensors for smart farming. Each case illustrates the promise of technology to drive growth, but also the peril of rights abuses, from algorithmic discrimination to mass surveillance. [689] [690]

At the global level, frameworks such as the GDPR in Europe, California's CCPA, and China's PIPL are redefining expectations for corporate accountability and user rights. African regulators must grapple with how to adapt these models without stifling local innovation or reinforcing dependency on foreign standards. This tension underscores the continent's strategic crossroads: either it develops context-sensitive approaches to compliance that foster trust, or risks becoming a passive consumer of technologies designed elsewhere. [691] [692] [693]

From a business perspective, compliance is often misunderstood as a check-box exercise to avoid sanctions. Yet evidence shows that firms with strong compliance cultures perform better in global markets. Paystack, a Nigerian fintech acquired by Stripe in 2020, explicitly credits its compliance posture as a key factor in its ability to expand across borders. [2] This suggests that, far from being a drag on competitiveness, rights-based compliance can serve as a differentiator in crowded digital markets. [694] [695]

Civil society and academia also play pivotal roles. Nigerian NGOs such as Paradigm Initiative have consistently highlighted privacy violations by state and private actors, pushing for stronger accountability. Meanwhile, African scholars argue that digital rights must be framed within the continent's socio-economic realities, not simply imported from Europe or North America. For example, Dr. Bright Simons, a Ghanaian technology entrepreneur, notes that Africa's "digital

---

[688] Andrew Crane and Dirk Matten, Business Ethics: Managing Corporate Citizenship and Sustainability in the Age of Globalization (Oxford: Oxford University Press, 2016).
[689] South Africa Information Regulator, "Media Statement on Facial Recognition Investigations," 2021.
[690] Office of the Data Protection Commissioner (Kenya), Annual Report 2022.
[691] Andrew Crane and Dirk Matten, Business Ethics: Managing Corporate Citizenship and Sustainability in the Age of Globalization (Oxford: Oxford University Press, 2016).
[692] State of California, California Consumer Privacy Act (CCPA), 2018.
[693] National People's Congress of China, Personal Information Protection Law (PIPL), 2021.
[694] Stripe, "Why We Acquired Paystack," Stripe Newsroom, October 2020.
[695] Andrew Crane and Dirk Matten, Business Ethics: Managing Corporate Citizenship and Sustainability in the Age of Globalization (Oxford: Oxford University Press, 2016).

sovereignty" depends not only on protecting rights but also on building the local capacity to process and govern its data. [3] [696] [697]

This article situates Nigeria's NDP Act within this broader landscape of technological disruption and regulatory evolution. It argues that compliance should be reframed not as a bureaucratic obligation but as a **strategic enabler of trust, innovation, and rights protection**. By comparing Nigeria's trajectory with other African examples (South Africa, Kenya) and global precedents (EU, U.S., China), the article develops a **four-pillar framework** for aligning compliance and rights: regulatory agility, corporate accountability, capacity building, and collaborative ecosystems. [698] [699] [700]

Ultimately, Africa faces a moment of destiny. Emerging technologies can deepen inequality and exploitation if left unchecked, or they can help create resilient, inclusive digital futures if grounded in rights-centered compliance. The choices Nigeria and other African states make in the coming years will shape not only domestic digital economies but also Africa's standing in the global information order. [701]

2.0 Literature Review & Conceptual Framework

2.1 Surveillance, Code, and Regulation

The intersection of rights, compliance, and technology has been a central concern of global scholarship for decades. Shoshana Zuboff's theory of surveillance capitalism argues that corporations increasingly treat personal data as raw material for behavioral prediction and profit, often at the expense of autonomy and democracy. In Africa, where mobile connectivity drives digital services, the extraction of personal data is not abstract it is embedded in everyday practices like mobile lending apps that collect excessive permissions from users' phones. [702] [703]

2.2 Lawrence Lessig's famous dictum "code is law" remains equally relevant. It suggests that technological architectures algorithms, platforms, and standards shape behavior as powerfully as statutes. In Nigeria, for example, the architecture of mobile payment apps can either protect or undermine privacy depending on default settings and encryption standards. This insight is vital for African regulators who must grapple not only with passing laws but also with ensuring that technological design aligns with rights. [704]

---

[696] Bright Simons, "Digital Sovereignty in Africa: The Road Ahead," IMANI Center for Policy and Education Report, 2021.
[697] Paradigm Initiative, "Annual Digital Rights in Africa Report," 2022.
[698] Andrew Crane and Dirk Matten, Business Ethics: Managing Corporate Citizenship and Sustainability in the Age of Globalization (Oxford: Oxford University Press, 2016).
[699] South Africa Information Regulator, "Media Statement on Facial Recognition Investigations," 2021.
[700] Office of the Data Protection Commissioner (Kenya), Annual Report 2022.
[701] Andrew Crane and Dirk Matten, Business Ethics: Managing Corporate Citizenship and Sustainability in the Age of Globalization (Oxford: Oxford University Press, 2016).
[702] Shoshana Zuboff, The Age of Surveillance Capitalism (New York: PublicAffairs, 2019).
[703] Andrew Crane and Dirk Matten, Business Ethics: Managing Corporate Citizenship and Sustainability in the Age of Globalization (Oxford: Oxford University Press, 2016).
[704] Lawrence Lessig, Code and Other Laws of Cyberspace (New York: Basic Books, 1999).

2.3 Compliance as a Legal Strategy?

Compliance is traditionally framed as a legal requirement: aligning with rules like the Nigeria Data Protection Act (NDP Act), South Africa's Protection of Personal Information Act (POPIA), or the European Union's GDPR. Yet scholars in business ethics and strategy stress a broader view: compliance can serve as a strategic enabler. By embedding rights-based practices into operations, firms build reputational capital, attract global partners, and reduce long-term risks.[3] [705] [706]

This strategic dimension is visible in African case studies. The Nigerian fintech Flutterwave, for instance, invests heavily in compliance to satisfy global investors and regulators. Meanwhile, smaller Nigerian SMEs often perceive audits under the NDP Act as a financial burden, revealing a compliance gap between resource-rich firms and under-capitalised businesses. [707]

2.4 Responsible Innovation [708]

A useful lens for bridging this gap is **responsible innovation (RI)**, which emphasises inclusivity, anticipation, reflexivity, and responsiveness in deploying technologies.[4] RI insists that technological choices must involve diverse stakeholders, anticipate potential harms, reflect on ethical dimensions, and adapt to feedback. Applied to data governance in Africa, this approach would mean involving civil society, regulators, and businesses in shaping standards around AI, IoT, and biometrics.

For instance, Kenya's Data Protection Commission has consulted NGOs when drafting digital credit rules, while Nigeria's NDPC has begun holding stakeholder consultations. Though still limited, these efforts align with RI principles, showing how compliance can evolve through collaborative processes rather than top-down imposition. [709] [710]

2.5 Towards a Conceptual Framework

Drawing from these insights, this article advances a **four-pillar framework** for aligning compliance with rights in Africa's digital economy: [711]

1. **Regulatory Agility** – Adaptive, technology-neutral laws that respond to evolving risks.
2. **Corporate Accountability** – Embedding compliance into governance, with leadership oversight. [712]

---

[705] Andrew Crane and Dirk Matten, Business Ethics: Managing Corporate Citizenship and Sustainability in the Age of Globalization (Oxford: Oxford University Press, 2016).
[706] South Africa Information Regulator, "Media Statement on Facial Recognition Investigations," 2021.
[707] Andrew Crane and Dirk Matten, Business Ethics: Managing Corporate Citizenship and Sustainability in the Age of Globalization (Oxford: Oxford University Press, 2016).
[708] René von Schomberg, "Prospects for Technology Assessment in a Framework of Responsible Research and Innovation," in Responsible Innovation: Managing the Responsible Emergence of Science and Innovation in Society, ed. Richard Owen et al. (Chichester: Wiley, 2013).
[709] Andrew Crane and Dirk Matten, Business Ethics: Managing Corporate Citizenship and Sustainability in the Age of Globalization (Oxford: Oxford University Press, 2016).
[710] Office of the Data Protection Commissioner (Kenya), Annual Report 2022.
[711] Andrew Crane and Dirk Matten, Business Ethics: Managing Corporate Citizenship and Sustainability in the Age of Globalization (Oxford: Oxford University Press, 2016).
[712] Andrew Crane and Dirk Matten, Business Ethics: Managing Corporate Citizenship and Sustainability in the Age of Globalization (Oxford: Oxford University Press, 2016).

3. **Capacity Building** – Providing SMEs, regulators, and civil society with technical skills and resources.
4. **Collaborative Ecosystems** – Fostering dialogue among regulators, firms, academia, and advocacy groups.

This framework recognizes that Africa's digital future cannot be secured by law alone. Compliance must be conceived as a living process, shaped by local realities yet attentive to global standards. In doing so, African voices scholars, entrepreneurs, regulators become central to shaping a digital order that protects rights without stifling innovation.

3.0 Emerging Technologies & Data Challenges

Emerging technologies in Africa's digital economy present both opportunities for growth and risks to rights. Four areas are particularly relevant: Artificial Intelligence (AI), Internet of Things (IoT), Blockchain, Fintech, and Biometrics.

3.1 Artificial Intelligence (AI)

AI is transforming sectors from finance to healthcare. Nigerian fintechs already use AI for fraud detection and credit scoring. Yet AI raises fairness concerns: biased training data can exclude women, rural populations, or informal workers from access to credit. Globally, the U.S. COMPAS algorithm in criminal justice has shown how predictive systems can reinforce discrimination. [5] For Africa, where datasets often reflect colonial-era inequalities, unchecked AI risks deepening socio-economic divides. [713]

The EU's Artificial Intelligence Act, which classifies "high-risk" AI systems and imposes strict transparency obligations, offers useful lessons. Nigerian regulators could adapt similar risk-based approaches, mandating fairness audits for fintech and recruitment AI systems. Such oversight would not stifle innovation but ensure AI serves inclusive growth.

3.2 Internet of Things (IoT)

IoT adoption is rising, from smart meters in Lagos estates to digital agriculture tools in East Africa. These devices collect vast amounts of real-time personal and behavioral data, often without user knowledge. Without robust cybersecurity, IoT devices can be hacked, exposing sensitive information or enabling unauthorised surveillance.

In Nigeria, telecom firms experimenting with smart city solutions must address these risks before scaling. Regionally, Kenya's digital agriculture programs show IoT's promise in boosting yields but also highlight dangers of exploitative contracts where farmers lose control of their data. African regulators need security-by-design standards to govern IoT rollouts. [714]

---

[713] Julia Angwin et al., "Machine Bias," ProPublica, May 23, 2016.
[714] Office of the Data Protection Commissioner (Kenya), Annual Report 2022.

3.3 Blockchain and Fintech

Blockchain underpins much of Africa's fintech innovation, from mobile money platforms to cross-border remittances. While it promises transparency, its pseudonymous design complicates enforcement of rights such as the "right to be forgotten." Nigerian regulators face the dual challenge of encouraging fintech growth while ensuring compliance with anti-money laundering (AML) and data protection obligations. [715]

Globally, regulators such as the U.S. SEC have clamped down on non-compliant crypto exchanges, signaling that decentralization does not exempt firms from oversight. For Nigeria, where fintech contributes significantly to GDP, clear but flexible blockchain regulation is essential for attracting investment while safeguarding consumer rights.

3.4 Biometrics

Biometric systems, -fingerprints, iris scans, and facial recognition are increasingly central to identity verification in Africa. Nigeria's National Identity Number (NIN) system links biometric data to banking, telecoms, and government services. While this enhances efficiency, it creates high-value targets for hackers and raises concerns about state surveillance.

South Africa offers a cautionary precedent: in 2021, its Information Regulator investigated banks' use of facial recognition under POPIA, signaling that even advanced economies face biometric risks. [6] In Nigeria, civil society groups have criticised weak safeguards around biometric databases, warning that breaches could undermine public trust in digital governance. [716]

3.5 Balancing Innovation and Risk

These four technologies illustrate the dual-edged nature of innovation: they enable economic growth but also magnify risks of privacy invasion, exclusion, and surveillance. For Nigeria and Africa more broadly, the challenge is to adopt risk-based, rights-centered governance. This means embedding data protection impact assessments (DPIAs) into business processes, promoting algorithmic transparency, and ensuring inclusive stakeholder input before large-scale deployments.

If managed responsibly, AI, IoT, blockchain, and biometrics can drive Africa's competitiveness in the global digital economy. If neglected, they risk reproducing inequalities and eroding trust in technology altogether.

4.0 Business and Compliance Dynamics

4.1 Compliance as Strategy

In Nigeria's digital economy, firms that treat compliance as more than a legal checkbox enjoy stronger reputations and market advantages. Compliance with frameworks like the Nigeria Data Protection Act (NDP Act) signals trustworthiness to consumers, investors, and global partners.

---

[715] Andrew Crane and Dirk Matten, Business Ethics: Managing Corporate Citizenship and Sustainability in the Age of Globalization (Oxford: Oxford University Press, 2016).
[716] South Africa Information Regulator, "Media Statement on Facial Recognition Investigations," 2021.

For instance, Paystack's early adoption of global compliance standards (e.g., PCI-DSS for payment security) made it attractive to Stripe, which acquired the company in 2020.[7] By embedding compliance into strategy, businesses reduce litigation risk, attract investment, and expand beyond Nigeria's borders. [717] [718]

4.2 Compliance Costs and Challenges

Yet, for many businesses especially SMEs compliance is seen as a costly burden. Data audits, staff training, and cybersecurity upgrades demand resources often unavailable to small firms. Nigeria's fragmented enforcement landscape compounds this problem. Some organisations enforce audits aggressively, while others lack capacity, creating uncertainty for businesses. Without consistent guidance and incentives, compliance risks becoming superficial "box-ticking" rather than genuine safeguards. [719]

Cultural attitudes also play a role. Many Nigerian consumers undervalue privacy, willingly sharing personal data for discounts or convenience. This weakens pressure on businesses to comply, unlike in Europe where consumer activism has driven accountability. Unless awareness grows, compliance will remain uneven. [720]

4.3 Global Regulatory Spillovers

Africa's businesses are shaped not only by domestic rules but also by extraterritorial frameworks like the European Union's GDPR. Nigerian airlines, fintechs, and universities that handle EU citizens' data must comply with GDPR or face fines. This global spillover is significant: firms seeking to serve diaspora markets must operate at international standards, regardless of local enforcement. Similarly, U.S. sectoral rules (like HIPAA for health data) and China's PIPL emphasize how global markets impose indirect compliance obligations on African firms. [721] [722] [723]

4.4 Business Incentives and Digital Trust

Surveys show that Nigerian consumers are becoming more cautious about how their data is used, especially after scandals involving telecom data sharing and election campaigns. Businesses that proactively disclose data practices and offer transparency tools such as consent dashboards can differentiate themselves. In competitive industries like fintech, where switching costs are low, trust becomes a powerful asset.

---

[717] Stripe, "Why We Acquired Paystack," Stripe Newsroom, October 2020.
[718] Andrew Crane and Dirk Matten, Business Ethics: Managing Corporate Citizenship and Sustainability in the Age of Globalization (Oxford: Oxford University Press, 2016).
[719] Andrew Crane and Dirk Matten, Business Ethics: Managing Corporate Citizenship and Sustainability in the Age of Globalization (Oxford: Oxford University Press, 2016).
[720] Andrew Crane and Dirk Matten, Business Ethics: Managing Corporate Citizenship and Sustainability in the Age of Globalization (Oxford: Oxford University Press, 2016).
[721] Andrew Crane and Dirk Matten, Business Ethics: Managing Corporate Citizenship and Sustainability in the Age of Globalization (Oxford: Oxford University Press, 2016).
[722] U.S. Department of Health & Human Services, Health Insurance Portability and Accountability Act of 1996 (HIPAA).
[723] National People's Congress of China, Personal Information Protection Law (PIPL), 2021.

4.5 Case for Compliance as Investment

The private sector thus faces a choice: treat compliance as a short-term cost or as a long-term investment. Firms that invest in compliance infrastructure not only reduce risk but also position themselves for cross-border expansion. In Africa, where regional integration (e.g., AfCFTA) is expanding, harmonised compliance could allow Nigerian firms to scale more easily across borders. Conversely, those that ignore compliance risk fines, reputational damage, and exclusion from global markets. [724]

5.0 Case Studies: Local, Regional, and Global Voices

5.1 Nigeria: NDPR and NDP Act Enforcement

Nigeria's data protection journey began with the Nigeria Data Protection Regulation (NDPR) of 2019, later replaced by the Nigeria Data Protection Act (NDP Act) of 2023. Enforcement has been uneven but symbolically important. In 2020, a major Nigerian bank was fined ₦5 million for unauthorised disclosure of customer data small by global standards but a clear signal of regulatory intent. Telecom operators have also been audited, showing that Nigeria's Data Protection Commission seeks to embed accountability despite resource constraints. For Nigerian firms, this means compliance is no longer optional. [725] [726]

5.2 Regional Africa: Kenya and South Africa [727] [728]

Kenya has positioned itself as a regional leader in digital rights. Its Office of the Data Protection Commissioner (ODPC) has investigated and deregistered digital lenders that used abusive data-driven debt collection practices. This demonstrates proactive enforcement to protect citizens from exploitation in fintech. [729]

South Africa provides another strong precedent. Under its Protection of Personal Information Act (POPIA), the Information Regulator fined the Department of Justice for failing to renew essential cybersecurity licenses. In 2021, it also investigated banks' use of facial recognition technologies. These cases highlight that even state agencies and powerful corporations can be held accountable, an example other African states can follow. [730] [731]

5.3 ECOWAS and the African Union

At the regional level, the African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention) provides a framework for harmonization. However, ratification

---

[724] Andrew Crane and Dirk Matten, Business Ethics: Managing Corporate Citizenship and Sustainability in the Age of Globalization (Oxford: Oxford University Press, 2016).
[725] Andrew Crane and Dirk Matten, Business Ethics: Managing Corporate Citizenship and Sustainability in the Age of Globalization (Oxford: Oxford University Press, 2016).
[726] Nigeria Data Protection Bureau, "Press Release on Bank Sanctions," 2020.
[727] South Africa Information Regulator, "Media Statement on Facial Recognition Investigations," 2021.
[728] Office of the Data Protection Commissioner (Kenya), Annual Report 2022.
[729] Office of the Data Protection Commissioner (Kenya), Annual Report 2022.
[730] South Africa Information Regulator, "Media Statement on Facial Recognition Investigations," 2021.
[731] South Africa Information Regulator, "Fine Against Department of Justice," 2021.

remains limited, slowing continent-wide adoption. ECOWAS has encouraged member states to align their laws, but progress varies: Nigeria has moved forward with the NDP Act, Ghana continues refining its Data Protection Act, while Senegal lags in enforcement. This unevenness creates risks of regulatory arbitrage, where firms exploit weaker jurisdictions. A harmonised regime could foster digital trade under the African Continental Free Trade Area (AfCFTA).

5.4 Global Precedents

Globally, regulatory precedents provide cautionary lessons. The EU's GDPR has levied multibillion-euro fines against companies like Meta (€1.2 billion in 2023) and Google (€50 million in 2019), showing the financial stakes of non-compliance. The U.S., in contrast, relies on fragmented sectoral rules like HIPAA for health data or CCPA in California. Meanwhile, China's Personal Information Protection Law (PIPL) asserts state sovereignty over data, signaling a different philosophy. [732] [733] [734] [735] [736] [737]

These global models shape African debates: Should Nigeria follow the EU in emphasizing rights, the U.S. in sectoral pragmatism, or China in state control? Each path has implications for innovation, investment, and rights protection.

5.5 Lessons for Africa

Case studies across local, regional, and global contexts highlight one reality: data protection is no longer optional. Nigeria and its peers must enforce compliance consistently while learning from stronger jurisdictions. Otherwise, weak enforcement will leave African citizens vulnerable and African businesses at a competitive disadvantage. [738]

6.0 Safeguarding Rights in a Digital Economy

The rise of Nigeria's digital economy creates vast opportunities, but it also heightens risks of exploitation, exclusion, and abuse. Safeguarding rights requires a deliberate balance between innovation and protection.

6.1 Privacy as a Fundamental Right

Privacy is not simply a Western construct; it has deep resonance in African traditions of dignity and communal respect. Under the Nigeria Data Protection Act (NDP Act 2023), individuals now enjoy clearer rights to know how their data is collected, processed, and shared. For example,

---

[732] Andrew Crane and Dirk Matten, Business Ethics: Managing Corporate Citizenship and Sustainability in the Age of Globalization (Oxford: Oxford University Press, 2016).
[733] European Data Protection Board, "EDPB Binding Decision 1/2023 on Meta Platforms Ireland Limited," 2023.
[734] European Data Protection Board, "Decision on Google LLC," 2019.
[735] U.S. Department of Health & Human Services, Health Insurance Portability and Accountability Act of 1996 (HIPAA).
[736] State of California, California Consumer Privacy Act (CCPA), 2018.
[737] National People's Congress of China, Personal Information Protection Law (PIPL), 2021.
[738] Andrew Crane and Dirk Matten, Business Ethics: Managing Corporate Citizenship and Sustainability in the Age of Globalization (Oxford: Oxford University Press, 2016).

citizens can demand deletion of their information if it is no longer necessary—a safeguard against indefinite surveillance. However, many Nigerians remain unaware of these rights, leaving them vulnerable to data misuse by both government agencies and private firms.

6.2 Equity and Digital Inclusion

A just data economy must avoid replicating existing inequalities. Rural Nigerians, women, and persons with disabilities risk being excluded if consent practices, digital tools, or literacy requirements are too complex. For instance, fintech platforms often require smartphone access and digital IDs, yet millions remain unbanked or undocumented. Without intentional policies, these groups may face "digital redlining", where services bypass them entirely. Bridging this gap means simplifying consent forms, expanding community digital literacy, and ensuring that marginalised voices shape regulatory frameworks.

6.3 Transparency and Accountability

Transparency builds trust. Nigerian businesses often adopt opaque data practices, burying terms of service in lengthy documents few can understand. To safeguard rights, firms must have an easy-to-read policy that states: why data is collected, who it is shared with, and for how long. Regulators like the Nigeria Data Protection Commission (NDPC) must push for Privacy by Design, making transparency a built-in feature rather than an afterthought. Civil society groups can also play a role by monitoring compliance and exposing malpractice. [739]

6.4 The Role of Civil Society and Media

Civil society remains crucial in defending rights. Advocacy organisations such as Paradigm Initiative have campaigned against unlawful surveillance and raised awareness of data rights. Independent media investigations have exposed cases of unauthorised SIM card registration and election-related data misuse. These interventions demonstrate that safeguarding rights requires more than laws, it demands active citizen oversight. [740]

6.5 Global Connections, Local Realities

Internationally, rights-based approaches under the EU's GDPR have strengthened individuals' control over their data, while in China, surveillance-heavy practices highlight the dangers of unchecked state power. Nigeria must chart a middle path: enabling innovation while protecting citizens. The African Charter on Human and Peoples' Rights already recognises the right to dignity and privacy Nigeria's challenge is to translate these principles into daily digital life.

---

[739] Andrew Crane and Dirk Matten, Business Ethics: Managing Corporate Citizenship and Sustainability in the Age of Globalization (Oxford: Oxford University Press, 2016).

[740] Paradigm Initiative, "Annual Digital Rights in Africa Report," 2022.

6.6 Looking Forward

Safeguarding rights in Nigeria's digital economy requires joint responsibility: regulators enforcing compliance, businesses prioritizing ethics, and citizens demanding accountability. If successful, Nigeria can set a precedent for Africa, proving that digital growth and rights protection are not contradictory but mutually reinforcing. [741]

7.0 Challenges, Risks, and Ethical Dilemmas

As Nigeria advances toward a data-driven economy, it faces persistent challenges that test the effectiveness of regulation, corporate responsibility, and citizen trust. These challenges highlight the tension between innovation and rights protection.

7.1 Cybercrime and Data Breaches

Nigeria's reputation as a hub for online fraud has shifted over the years, from "419" scams to sophisticated cybercrime targeting banks, telecoms, and even government systems. Recent cases of SIM swap fraud illustrate how criminals exploit weak identity verification systems to drain victims' accounts. Data breaches, whether through poor security or insider leaks, also erode trust in digital services. Weak reporting culture makes the situation worse, as companies often hide breaches to protect their reputation.

7.2 Surveillance and Privacy Concerns

The expansion of surveillance tools by both state and private actors raises serious ethical dilemmas. Initiatives like SIM card registration, national identity databases, and CCTV expansion are often justified on grounds of security but risk sliding into mass surveillance without adequate safeguards. Citizens worry about who has access to their personal data and whether it could be misused for political or commercial purposes. The tension between national security and personal freedom remains unresolved.

7.3 Weak Enforcement and Compliance Gaps

Despite the Nigeria Data Protection Commission (NDPC) being established to enforce compliance, enforcement remains inconsistent. Many small and medium enterprises (SMEs) see data protection as a luxury, not a necessity. Large corporations may adopt privacy policies, but often only for optics, with limited internal monitoring. This enforcement gap risks turning Nigeria's data protection framework into a "paper tiger" impressive in theory but weak in practice. [742]

---

[741] Andrew Crane and Dirk Matten, Business Ethics: Managing Corporate Citizenship and Sustainability in the Age of Globalization (Oxford: Oxford University Press, 2016).
[742] Andrew Crane and Dirk Matten, Business Ethics: Managing Corporate Citizenship and Sustainability in the Age of Globalization (Oxford: Oxford University Press, 2016).

7.4 Ethical Dilemmas in Innovation

Fintech, healthtech, and EdTech platforms are fueling rapid innovation, but they also raise ethical questions. Should fintech apps use behavioural nudging to drive spending and borrowing, or should they prioritise financial well-being? Should health platforms collect genetic or biometric data if users don't fully understand the risks? Innovation in these sectors is vital for growth, yet unchecked practices risk exploiting vulnerable populations.

7.5 Inequality and Digital Exclusion

A significant dilemma lies in balancing digital expansion with inclusion. Many rural Nigerians still lack reliable internet access, meaning they are excluded from digital financial systems, e-governance, and education platforms. Ethical concerns arise when urban elites benefit disproportionately while rural citizens bear the risks of surveillance without enjoying the benefits of connectivity.

7.6 Trust Deficit

The underlying challenge across all these issues is trust. Citizens are skeptical of both corporations and government institutions handling their data. Without trust, even well-designed systems will struggle to gain adoption, whether it's digital ID programs, e-voting platforms, or open banking initiatives.

7.7 Path Forward

Nigeria must strengthen enforcement, promote corporate accountability, and ensure citizen-centered innovation. Cybersecurity frameworks must be enhanced, and stronger penalties for data breaches enforced. More importantly, policies should be guided by ethics, ensuring innovation never tramples on rights.

8.0 Recommendations & Way Forward

To build a sustainable, rights-based digital economy, Nigeria must move beyond compliance checklists and embrace a holistic approach that blends regulation, innovation, ethics, and citizen empowerment. The following recommendations outline a path forward: [743]

8.1 Strengthen Enforcement Capacity

The Nigeria Data Protection Commission (NDPC) must be equipped with stronger legal, financial, and technical resources. Beyond issuing fines, the Commission should develop sector-specific

[743] Andrew Crane and Dirk Matten, Business Ethics: Managing Corporate Citizenship and Sustainability in the Age of Globalization (Oxford: Oxford University Press, 2016).

compliance guidelines, enhance whistleblower protection, and establish fast-track mechanisms for reporting and resolving breaches. [744]

8.2 Promote Corporate Accountability

Businesses must view data protection as a strategic advantage, not just a regulatory burden. Adoption of Privacy by Design principles, data minimisation, and transparent consent processes should become industry norms. Mandatory Data Protection Impact Assessments (DPIAs) for high-risk projects, such as AI-based lending or biometric verification will ensure accountability before harm occurs.

8.3 Embed Ethics in Innovation

Innovation in fintech, healthtech, EdTech, and e-governance must be guided by ethics frameworks that prioritise human dignity, fairness, and inclusion. Tech startups should adopt voluntary codes of ethics alongside compliance standards, ensuring technology serves the people rather than exploiting them. [745]

8.4 Enhance Public Awareness and Digital Literacy

Citizens are the ultimate custodians of their data, but only if they understand their rights. National campaigns, school curricula, and civil society-led training programs should promote digital literacy, teaching Nigerians how to protect their privacy, identify scams, and demand accountability from institutions.

8.5 Balance Security and Privacy

National security measures—such as surveillance and biometric databases—must be balanced with robust safeguards. This includes independent oversight, judicial review mechanisms, and limits on data retention. Transparency reports from both government and corporations will foster greater trust.

8.6 Foster Regional and Global Collaboration

Nigeria should actively collaborate with other African countries through the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) and with global partners to harmonise standards. This will facilitate cross-border trade, data flows, and digital trust in Africa's emerging single digital market.

---

[744] Andrew Crane and Dirk Matten, Business Ethics: Managing Corporate Citizenship and Sustainability in the Age of Globalization (Oxford: Oxford University Press, 2016).
[745] Andrew Crane and Dirk Matten, Business Ethics: Managing Corporate Citizenship and Sustainability in the Age of Globalization (Oxford: Oxford University Press, 2016).

8.7 Prioritise Inclusion and Equity

Digital policies must address the rural-urban divide. Subsidised broadband access, public Wi-Fi in underserved regions, and digital ID systems that work offline will ensure that data rights are **equitably protected**. Without inclusion, data governance risks reinforcing inequality.

8.8 Establish Independent Oversight and Multi-Stakeholder Engagement

Finally, a multi-stakeholder council comprising regulators, private sector, civil society, academia, and citizen representatives should be institutionalised to monitor implementation, advise on ethical dilemmas, and ensure that Nigeria's data protection framework evolves with global trends.