

Paper

Privacy by Design in Early-Stage Innovation:

How Data Protection
Advances AI-Driven
DPI in Nigeria



digital
impact
alliance

Foreword

Nigeria's vibrant startup ecosystem has positioned the country as a major technology hub in Africa with five of Africa's unicorns originating from Nigeria. This burgeoning growth and Nigeria's vibrant population of over 230 million data subjects yields an unprecedented volume of data, driving digital transformation to address socio-economic issues. It is therefore imperative to sustainably manage this essential resource, to propel economic growth, and safeguard the fundamental rights and freedoms of data subjects as guaranteed under the Constitution of the Federal Republic of Nigeria, 1999.

This White Paper chronicles the Nigeria Data Protection Commission's (the Commission) approach to ensuring responsible innovation, in collaboration with the Digital Impact Alliance (DIAL). What started out as a regulatory task became a test case in adopting a balanced approach to regulation and innovation. The Commission's collaborative effort successfully fulfilled the third pillar of the Commission's Strategic Roadmap and Action Plan (2023–2027), which focuses on Collaboration and Co-operation, while simultaneously advancing the mandatory adoption of privacy-by-design principles. It also underscored the Commission's objective of effectively ensuring compliance while encouraging responsible innovation. The outcome of this collaboration confirms the Commission's position that robust data privacy standards form the bedrock of trusted and secure innovation.

The Commission is proud to co-author this paper with DIAL, marking a significant milestone in our commitment to fostering a sustainable and trustworthy digital economy in Nigeria. The analysis provided in this white paper lays the groundwork for a more consultative and proactive regulatory future.

We are confident that the insights provided and the framework validated in this project will not only serve the Nigerian data protection landscape but also provide a scalable model for balancing regulatory oversight and technological acceleration across the African continent.

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

Executive Summary

Today, governments all over the world are embracing data and digital technology as a catalyst for change—driving efficiency, economic development, and social inclusion. As the pace of innovation accelerates, digital public infrastructure (DPI) presents an opportunity for governments to coalesce around a trusted, effective approach to designing, implementing, and governing foundational digital systems. These include digital identity (digital ID), digital payments, and data exchange systems—building blocks that, together, form the basis for countless digital tools, services, and solutions. When combined with artificial intelligence (AI), the benefits are even greater, promoting enhanced efficiency, decision-making, and accessibility.

To fully maximize the benefits of digital transformation—especially for inclusive economic and social growth—the right technical and policy frameworks must be in place. These include robust data protection policies as well as implementation frameworks that can guide both innovators and governments toward best and secure practices in data collection, sharing, and management. In Nigeria, many innovators face common challenges—including funding scarcity, lack of ecosystem maturity, and capacity gaps—which can hinder them from prioritizing these safeguards. Such barriers, when combined with the emergence of AI, result in both an urgent challenge and an opportunity to strengthen crucial data protection and governance measures.

To help realize this vision, the Digital Impact Alliance (DIAL) worked in a collaborative effort with the Nigeria Data Protection Commission (NDPC) to advance good practices around data protection and sharing. These serve to ensure privacy-by-design, empower innovators, and support the startup ecosystem. During this year-long joint project, DIAL and NDPC engaged with nine local innovators developing and piloting digital solutions to solve pressing real-world problems, including maternal mortality, affordable healthcare access, and financial inclusion. Through a combination of targeted workshops, communities of practice, and hands-on assessments, we worked to both educate the innovators on compliance and help them better understand and solve the challenges they faced in complying with the Nigeria Data Protection Act (2023) and other regulatory instruments issued by the NDPC.

This paper highlights key findings, insights, and takeaways from this work, exploring the importance of shared learning, collaboration, and capacity strengthening in advancing a strong data governance ecosystem.

Introduction & Context

Nigeria is a multi-ethnic and culturally diverse federation made up of 36 states and the Federal Capital Territory. With a population exceeding 220 million, it is both the largest economy and the most populous nation in Africa, and these attributes continue to shape its growing influence as a regional leader in technology and innovation. This scale and diversity have nurtured one of the continent's most vibrant digital ecosystems, positioning Nigeria as a leading hub for entrepreneurship and technological advancement. Over the past decade, the country has produced some of Africa's most recognized technology enterprises and unicorns, including Flutterwave, Interswitch, and Opay, underscoring its position as a powerhouse for digital enterprise and talent. Nigeria's eNaira represents another important milestone—the first Central Bank Digital Currency (CBDC) to officially launch in Africa back in 2021. Following Nigeria's lead, Ghana and South Africa have since piloted their own CBDCs, reflecting a broader continental push toward financial innovation and inclusion.

Nigeria's digital transformation has also gathered pace in terms of infrastructure. The number of mobile connections reached approximately 150 million by January 2025, equivalent to roughly 64% of the population. This growth has been reinforced by broadband expansion under the National Broadband Plan (2020–2025) and by large-scale connectivity projects such as Project BRIDGE, which aims to extend fibre coverage to 120,000 km nationwide. Together, these efforts are strengthening the backbone of a more connected and digitally empowered society.

Complementing these infrastructure gains are decisive policy and institutional reforms that have laid the groundwork for Nigeria's digital public infrastructure (DPI)¹ and set the stage for responsible innovation. The advent of AI into this mix introduces both new opportunities and risks. AI has the potential to build on DPI foundations to enable smarter, more adaptive solutions across multiple sectors—democratizing access through multilingual access,² trust through early fraud detection in the financial system,³ and in many other crucial ways. Yet, the same systems also heighten concerns around privacy, fairness, and transparency—especially when considered against the backdrop of low citizen trust in digital platforms.⁴

Digital Public Infrastructure (DPI) in Nigeria

Nigeria is actively pursuing the implementation of DPI to accelerate digital inclusion and efficiency in government service delivery. While progress is significant, maturity levels vary across the country.



Nigeria has established some of the core foundations for effective DPI deployment:

- a. **Digital ID:** The National Identity Management Commission (NIMC) continues to anchor Nigeria's identity ecosystem. As of June 2025, over 121 million National Identification Numbers (NIN) have been issued,⁵ establishing a crucial foundation for digital identity. The recent launch and rollout of the NIN Authentication Service⁶ (NINAuth) mandated for verification across all Ministries, Departments, and Agencies has strengthened the security and reliability of digital identity verification. NIMC has also migrated all telecommunications operators to the NINAuth platform and upgraded its diaspora enrolment system, enhancing both interoperability and inclusion within Nigeria's identity framework.
- b. **Digital Payments:** The payments layer of Nigeria's DPI ecosystem is among the most advanced on the continent. The Nigeria Inter-Bank Settlement System (NIBSS), jointly owned by the Central Bank of Nigeria (CBN) and licensed banks, operates the NIBSS Instant Payment (NIP) system that has transformed digital transactions since its launch in 2012, facilitating secure digital financial transactions.
- c. **Data Exchange:** Data exchange across the government remains in its early stages but is rapidly evolving. Data exchange between Ministries, Departments, and Agencies is currently nascent. While sectoral data exchanges exist—for example, between the Ministry of Health, the Ministry of Lands, and the Revenue Authority—cross-sectoral interoperability remains limited. However, to resolve this limitation, the Federal Ministry of Communications, Innovation and Digital Economy (FMCIDE) is currently working on the deployment of the Nigeria Data Exchange Platform (NGDX) to enable secure and seamless data exchange. It is scheduled to go live by the end of 2025.

Sub-National Maturity Assessment

A recent report published by the Nigeria Governors' Forum in July 2025⁷ revealed varying levels of digital maturity across states.

- a. **DPI Readiness:** Only two states demonstrated a high maturity level, while twenty states are at medium maturity, and twelve states fall under the low maturity category.

- b. Enabling environment:** The underlying environment needed for DPI adoption varies equally, with two states showing high maturity, twenty-two at medium maturity, and ten at a low maturity level.

AI Adoption in Nigeria

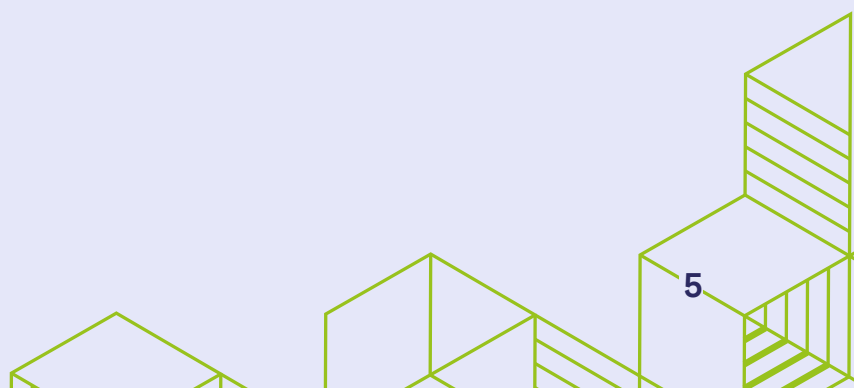
The country's vibrant innovation community plays a critical role in Nigeria's digital development. Today, Nigeria ranks second among African nations⁸ with over 400 AI firms and start-ups, following South Africa, which leads with about 600. Nigeria enjoys high levels of innovation, a diverse start-up sector, and strong political will. With the advent of generative AI, the potential for innovation is incredible, as AI-powered tools and solutions can increase productivity, foster inclusion, and overcome traditional development barriers.

To guide this emerging landscape, the FMCIDE released a National AI Strategy in 2024. Though not yet finalised, the document provides a guiding framework for innovators, academia, and government entities on the responsible use of AI.

At the same time, governments—including the Nigerian government, which has launched a national AI strategy and is putting institutional frameworks in place—remain among the most significant yet cautious adopters of AI.⁹ This caution is not mere bureaucracy; it reflects the public sector's responsibility to safeguard citizens' rights and ensure that technology serves the public interest. When deployed responsibly, AI can strengthen public sector performance by improving productivity, service delivery, and accountability. However, without clear frameworks, it can also heighten risks related to data protection, surveillance, and algorithmic bias. Striking the right balance between innovation and oversight is therefore essential to building public trust and ensuring that AI enhances, rather than undermines, the social contract between citizens and the state.

Data Protection

Spearheading the country's data protection efforts is the Nigeria Data Protection Commission (NDPC), an independent regulator for data protection and privacy issues. NDPC's main objective, among others, is to ensure the guidance and advancement of privacy-by-design principles for implementation across the country. Through this work, NDPC helps ensure digital solutions are ethical and trustworthy, leveraging data to solve socio-economic problems without compromising privacy rights.



In recent years, NDPC has led several key policy initiatives, which form the basis of Nigeria's data legislation landscape. These include:

1. **Nigeria Data Protection Regulation (NDPR), 2019¹⁰:** The first comprehensive regulation on data protection, issued under the National Information Technology Development Agency (NITDA), which provided initial compliance obligations for controllers and processors, as well as enforceable data subject rights. Though now transitional, it laid the groundwork for subsequent legislation.
2. **NDPR Implementation Framework, 2020¹¹:** A practical guide to operationalising the NDPR, detailing roles, procedures, and compliance obligations.
3. **Nigeria Data Protection Act (NDP Act), 2023¹²:** The first national law on data protection passed by the National Assembly, which formally established NDPC as the regulator for data protection and privacy issues, clarified data subjects' rights and obligations, and provided statutory backing to enforcement mechanisms.
4. **Nigeria Data Protection Act – General Application and Implementation Directive (NDP Act - GAID), 2025¹³:** NDPC's operational directive under the NDPA, issued to provide practical compliance guidance, directives, templates—such as the Data Protection Impact Assessment (DPIA) in Schedule 4—and transitional rules that phase out the application of the older NDPR framework.
5. **Supplementary Guidelines and Notices:** This includes sector-specific guidance, for example, guidance circulars for public institutions; codes of conduct; and compliance advisories, which help interpret and apply the law in practice.

Together, these policies and instruments reflect the NDPC's ongoing evolution and its commitment to translating theory into practice. The NDP Act serves as the legal foundation, while the NDP Act - GAID functions as the operational guide that brings the framework to life.

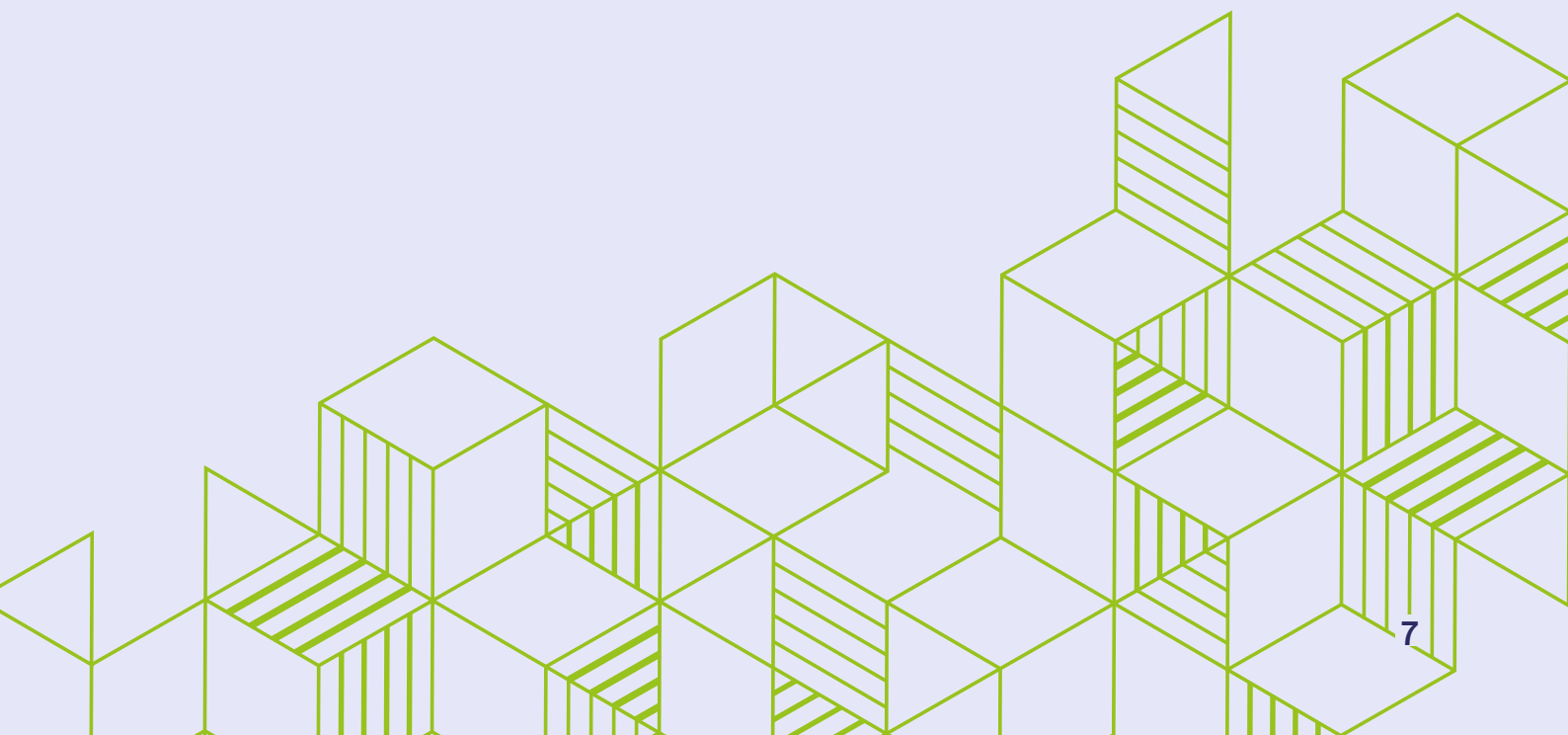
To raise awareness and educate the public on the obligations in these regulatory instruments, the NDPC actively engaged with key stakeholders—particularly within the startup ecosystem. This sector is a critical driver of digital transformation and AI development within Nigeria, and yet, they continue to face persistent challenges like funding, scarcity, capacity barriers, and organizational maturity.

With this recognition, in 2025, DIAL has been supporting nine local innovators to both address the barriers they experience in implementing effective data protection within their digital solutions, while also promoting greater understanding around these principles. NDPC, as the data protection regulator,

was approached to provide compliance education to the innovators, through which it highlighted the role of innovators as important players in advancing data protection in practice, while DIAL led coordination and ecosystem building efforts, bringing together key stakeholders, including state representatives, policymakers, and technical partners.

Through these efforts, NDPC aimed to demonstrate that embedding privacy-by-design principles early in the innovation process can yield tangible benefits: fostering greater trust in data protection, encouraging broader adoption, and establishing a clear model for integrating safeguards across emerging digital enterprises. For DIAL, this collaboration served as an opportunity to better understand the role that data protection plays as a fundamental component of harnessing the combined potential of AI and DPI.

Ultimately, NDPC's evolving approach reflects the dual responsibility of regulators—to both supervise and enable. By developing iterative frameworks and continuous-assessment mechanisms that accompany innovators through the lifecycle of their projects, NDPC is ensuring that compliance and innovation advance in tandem. This balanced stance—combining strategic oversight with practical support—positions Nigeria to strengthen its safeguards while sustaining momentum in the digital economy.



Approach

Given the objectives set out for NDPC, the agency is faced with both an opportunity and a challenge. On one hand, it must demonstrate how newly issued regulatory frameworks and initiatives translate in practice—particularly for early-stage innovators and public interest technology solutions that often operate with limited resources and capacity.

Against this backdrop, NDPC and DIAL launched a learning-focused project to explore how data protection principles can be meaningfully applied in real-world innovation settings. The objective of the project was to test how the Data Protection Impact Assessment (DPIA) framework under Schedule 4 of the NDP Act - GAID, could be operationalized, while uncovering the specific gaps the agency needs to address—looking through the lens of an innovator.

At the core of this collaboration was an understanding that this project was both a compliance exercise and a learning journey. The aim was not only to ensure that solutions piloted within this collaborative effort met the requirements of the recently issued directive, but also to test, refine, and embed NDPC's regulatory instruments in practice.

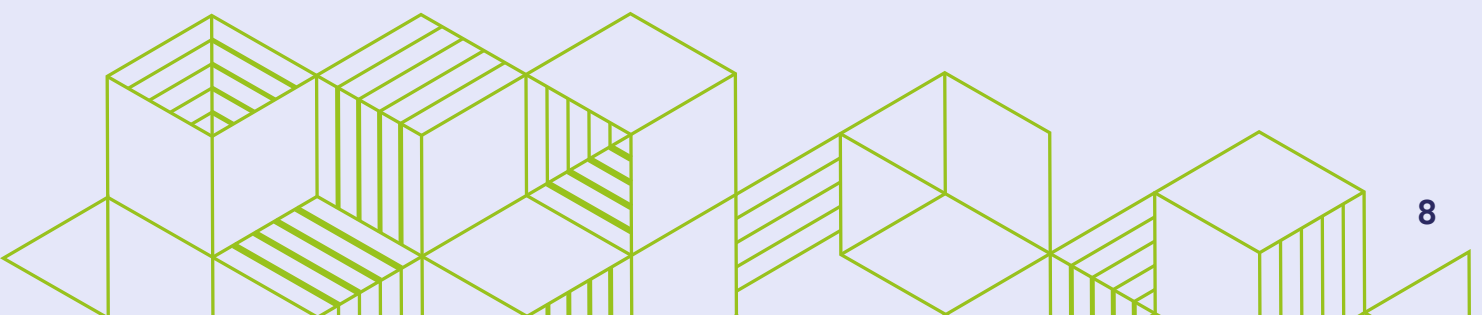
We approached this exercise with three guiding questions:

1. Could early-stage startups realistically use the new Data Protection Impact Assessment (DPIA) framework?
2. What kind of support would they need to internalize safeguards without stifling innovation?
3. How could NDPC, states across Nigeria, and development partners co-create an enabling environment that turns compliance into a driver of trust?

With these questions in mind, the project took form in six critical ways.

1. Test case for National Standards

The project began with the NDPC providing oversight for the DPIAs applied to the digital solutions proposed by the innovators. This coincided with the issuance of the official DPIA Template, issued as Schedule 4 to the NDP Act – GAID. The alignment created a timely opportunity to validate the framework not as



a theoretical instrument, but as a practical tool—tested directly by innovators working on live solutions.

As a result, NDPC received concrete, practice-based feedback on the practicality of its instrument, and how it guided the innovators in thinking of measures to embed safeguards in design to mitigate possible privacy risks in the solutions.

2. Hands-on orientation with the community of practice and innovators

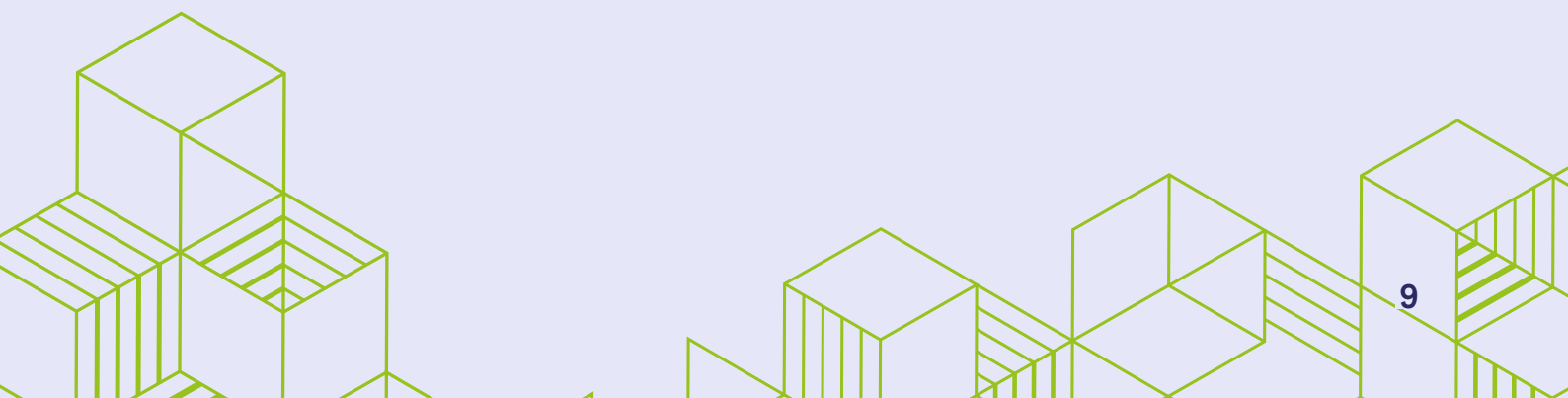
In March 2025, DIAL and NDPC organized a full-day structured session with a newly established Community of Practice (COP)—a network of state representatives from Kano, Kaduna, and Gombe to review the NDP Act and NDP Act - GAID framework in detail. This session set the stage for collaboration and political buy-in. In Nigeria's federal system, states are essential for implementation, so it was critical that they had confidence in knowing that innovators were considering compliance as part of their development process.

A subsequent session was convened during August 2025 with the cohort of innovators. Anchored by a representative from NDPC, the workshop guided participants through the NDP Act and each section of the DPIA template, unpacking technical and legal requirements and translating them into practical steps for product teams. This hands-on and iterative orientation strengthened innovators' capacity to manage their own compliance journey, while maintaining regulatory oversight that was supportive rather than punitive. Ultimately, this workshop enabled them to approach compliance with confidence and a sense of collaboration.

3. Practical DPIA development

Each innovator was required to draft their own DPIA using the NDPC template. These submissions were reviewed collaboratively by NDPC and DIAL experts, with constructive feedback loops introduced to improve clarity, compliance, and completeness.

This exercise reinforced the value of the DPIA as more than a compliance obligation; it became a design tool for embedding responsible innovation practices from the ground up. The assessment helped to shape key product decisions, as the innovators were able to revise solution features such as consent flows and data handling practices. Importantly, the process also generated practical feedback on the usability and depth of the template itself—insights that may inform future revisions to make the instrument more accessible and user-friendly.



4. Capacity building for long-term adoption

Beyond the one-off review exercise, the NDPC and DIAL teams delivered targeted training modules on both the NDP Act - GAID and DPIA frameworks. During these sessions, NDPC and DIAL also provided compliance checklists, supported innovators to nominate internal focal points, and assigned accredited Data Protection Officers (DPOs) to each innovator to review and standardize DPIA submissions after initial drafts.

Because startups often lack in-house legal or compliance expertise, embedding DPOs and practical tools reduces the burden, ensuring quality and consistency in compliance. This targeted support equipped the innovators with practical skills to integrate safeguards into their solutions and emphasized the principle of data protection by design. As a result, they produced higher-quality DPIAs, standardized across the cohort.

Ultimately, the sessions' focus on long-term adoption aimed to nurture a culture where compliance and innovation can advance hand in hand, sustaining safeguards well beyond the pilot phase.

5. Ongoing support and validation

Following the Bootcamp, the NDPC team continued to provide structured guidance to innovators, reviewing DPIA drafts, flagging gaps, and preparing teams for eventual validation. Because the innovators' sustained engagement was necessary to keep their startups on track, prevent compliance fatigue, and ensure that learnings translated into action, this support was key. It allowed product teams to remain focused on solution deployment while benefiting from dedicated, knowledgeable guidance through the DPIA process. Additionally, and most importantly, it allowed innovators to steadily improve their submissions while staying focused on deployment.

6. Collaborative ecosystem engagement

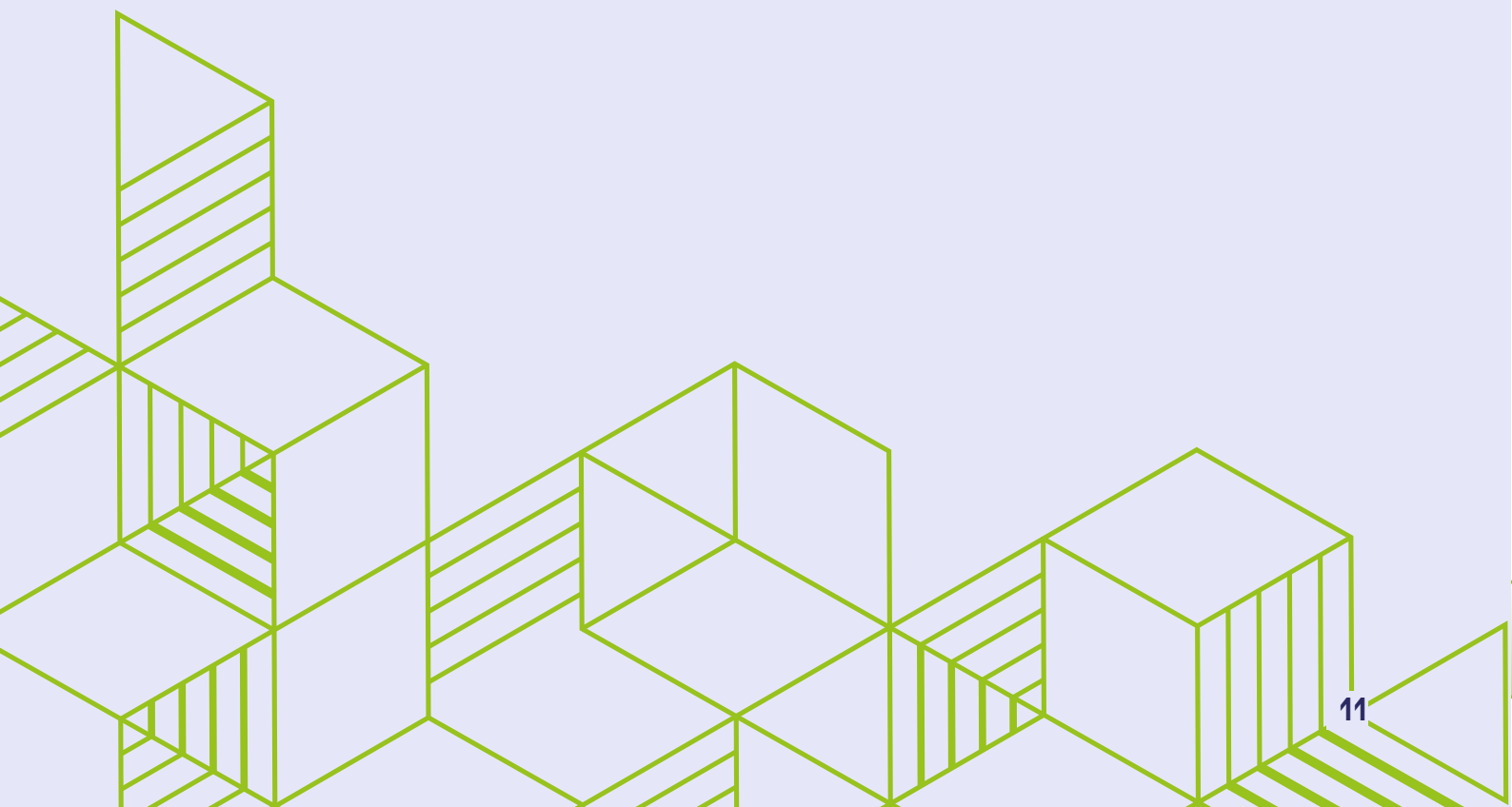
At every stage, DIAL and NDPC positioned the DPIA process not only as a compliance requirement but as a means of empowering the startup ecosystem. The collaboration between regulatory authorities, development partners, and innovators illustrated how safeguards can be co-created in ways that are both rigorous and innovation friendly.

Turning Potential into Progress

As of the last quarter of 2025, the project has progressed from framework validation into practical field deployment. Each innovator has completed a comprehensive DPIA using the NDPC template, and this process has proven invaluable in building trust across government stakeholders. Because the solutions have now passed through NDPC's regulatory review, state partners are more comfortable engaging with the innovators, confident that the products meet baseline data protection and compliance standards.

The innovators have also embarked on state visits to Kaduna, Kano, Gombe, and Lagos to situate their solutions within local contexts, align with state ministries and agencies, and prepare for pilot implementation scheduled to commence in November 2025. Importantly, NDPC registration and approval details will feature prominently within each solution, offering end users visible assurance that their data is being handled under regulatory oversight. This practical alignment of safeguards, government trust, and user confidence marks a pivotal step toward embedding responsible innovation within Nigeria's DPI ecosystem.

As a strategic partner, DIAL was able to bring convening power, neutrality, and resources—bridging the gaps between regulators and startups. These efforts built trust among the stakeholders involved and simultaneously enabled NDPC to advance data protection. This type of collaborative, hands-on approach to effective data governance is not only key to good DPI and AI design, but central to supporting Nigeria's broader digital innovation agenda.



Insights and Analysis

This project provided several key learnings into the state of Nigeria's data protection ecosystem, as well as opportunities for overcoming common challenges that innovators face.

1. Overcoming capacity barriers through creative means.

Because seven of the nine of the innovators came from start-up ecosystems, they had differing levels of maturity, bandwidth, and resources. To better support them throughout the process, DIAL nominated Data Protection Officers (DPO) to work with the innovators and fulfil their compliance obligation under the NDP Act. In addition to this targeted support, implementing a regulatory sandbox could also be effective in helping overcome capacity barriers and optimizing the DPIA process for low-resource organizations and innovators.

NDPC is currently working on a regulatory sandbox policy to provide innovators with an environment to work with regulators while building their solutions. This will provide the needed guidance required by innovators to ensure that privacy-by-design principles are embedded into solutions from their inception, particularly solutions that are being developed to solve socio-economic problems. Collaborating on this exercise with DIAL provided NDPC with practical insights that will enhance its regulatory sandbox policy and how this policy may be implemented in practice.

Across Africa, regulatory sandboxes have primarily emerged in the financial sector, where central banks and market regulators in countries such as Nigeria, Kenya, Ghana, South Africa, Rwanda, Uganda, and Sierra Leone have successfully deployed them to test fintech and digital-payment innovations under controlled, risk-managed conditions. These models have proven effective for enabling innovation while maintaining consumer protection, but they have largely remained sector-specific and finance-oriented.

By contrast, the NDPC's proposed sandbox represents one of the earliest efforts on the continent to extend the sandbox model into the data protection and AI governance space—creating a test environment focused on ethical data use, privacy-by-design, and responsible digital innovation. While the Datasphere Initiative has advanced a policy-oriented model of sandboxes as spaces for governance experimentation—helping countries explore agile and cross-sector approaches to data management—NDPC's concept is more regulatory and practice-driven, anchored in Nigeria's legal framework and designed to operationalize safeguards through live product testing.

There are also emerging global precedents, such as the United Kingdom Information Commissioner's sandbox for privacy-enhancing technologies.

However, there are very few documented regulatory sandboxes in Africa that focus explicitly on data governance and safeguards, rather than fintech. This positions NDPC's approach as a novel and forward-leaning initiative, bridging the gap between high-level policy experimentation and enforceable regulatory practice in the region.

Key takeaway: Considering support mechanisms that reduce the burden on startups can serve to advance both innovation and data protection measures.

2. Identifying common challenges.

When conducting the DPIA, a key challenge for the innovators was the availability of resources as well as the financial cost. Had it not been a core requirement of the project and as such, some support provided, the innovators would likely have been unable to prioritize it. This reality illustrates the need for greater resources, both by onboarding data protection officers and implementing sandboxes, which in the future could be a more cost-effective solution.

Key takeaway: Rethinking funding and payment structures could help promote greater prioritization of data protection in the future.

3. Adopting a collaborative approach to regulation.

Throughout the project, NDPC prioritized a collaborative, hands-on approach, rather than acting as a distant enforcer. The innovators responded positively to this active involvement, as it allowed them to see data protection as an enabler for their solutions, rather than another regulatory burden. By walking innovators through the NDP Act - GAID framework and the DPIA template, NDPC reframed compliance as a collaborative process.

Key takeaway: Regulators adopting a collaborative approach can accelerate adoption and reduce resistance, especially in emerging innovation ecosystems.

4. Embedding safeguards early.

Treating the DPIA not as a post-development requirement but as an integrated design step helped innovators anticipate risks from the outset. This approach shifted safeguards from being a late-stage burden into a core feature of product development.

For instance, one of the innovators used the DPIA process to identify data residency and sovereignty concerns early in the design phase. As a result, they began migrating their datasets to a local MTN data centre—ensuring compliance with national data protection principles and strengthening user trust. Another reported that possessing a completed DPIA, combined with their registration and recent audit with the NDPC, made it considerably easier to engage with government agencies. These credentials signalled seriousness and regulatory readiness, opening doors to collaborative discussions that would otherwise have been difficult to initiate.

Similarly, the Federal Competition and Consumer Protection Commission (FCCPC) has recently issued regulations requiring all digital and online lending platforms to obtain formal registration or clearance under its Digital, Electronic, Online or Non-Traditional Consumer Lending Regulations of July 21, 2025. Within this evolving regulatory environment, the completion of a robust DPIA positioned our innovators ahead of potential compliance risks. The DPIA process had already addressed many of the FCCPC's likely concerns—particularly those relating to informed user consent, data handling, and processing transparency. Consequently, engagements with the FCCPC proceeded more smoothly, as the DPIA served not only as a compliance framework but also as a trust-building instrument that demonstrated regulatory readiness and accountability.

Key takeaway: Positioning compliance tools like DPIAs as design instruments ensures that safeguards are embedded in innovation from the ground up. It also demonstrates that early regulatory alignment can yield tangible operational advantages—from easier engagement with public institutions to reduced friction with oversight bodies.

5. Embracing feedback as a policy driver.

The real-world application of the DPIA template surfaced practical insights about its usability and depth. Innovators' feedback highlighted areas where the template could be simplified or clarified, offering NDPC valuable input for future refinement.

Key takeaway: Embedding structured feedback loops into regulatory processes allows policies and tools to evolve in line with ecosystem realities.

6. Building confidence through early orientation.

Dedicating time at the outset to walk innovators and state representatives through the NDP Act - GAID framework made a significant difference. By demystifying technical and legal requirements, these sessions gave participants the confidence to approach compliance proactively rather than reactively.

Key takeaway: Investing in structured orientation at the beginning reduces uncertainty and equips innovators to internalize safeguards as part of their normal design process.

7. Responsible AI through structured governance.

During the early days of the project, it was clear that most innovators initially saw AI as purely a technical capability; the DPIA process reframed it as a governance and accountability exercise. Completing the DPIA compelled teams using AI models—for example, in credit scoring and health intervention severity scaling—to map out data flows and assess potential bias and exclusion (based on language for instance). This exercise exposed blind spots around model explainability, data availability, and user consent that may have gone unnoticed otherwise.

One of the strongest outcomes was the recognition that responsible AI begins with transparency. Innovators are now designing internal audit trails, fairness checks,

and considering subtle triggers in their models, ensuring that AI decisions can be explained and corrected when needed.

Key takeaway: Integrating AI considerations within the DPIA process transforms abstract ethics into operational safeguards. It ensures that models are not only accurate and efficient but also transparent, accountable, and aligned with Nigeria's data protection and consumer-rights principles.

Policy Recommendations

While every country's situation is unique, Nigeria's experience can provide important learnings and takeaways for governments, policymakers, and funders seeking to integrate data protection practices. The following recommendations are based upon key themes observed during the course of the project, including the importance of design decisions, technical support, and capacity strengthening.

Embed “Trust by Design” into innovation ecosystems.

When governments champion responsible data practices as a core aspect of innovation rather than as compliance at the finish line, they transform regulation into a signal of quality, trust, and readiness to scale. These design choices can include elements such as robust privacy settings, encryption and secure data storage, and consent mechanisms, which act as fundamental safeguards, build confidence in digital tools, and strengthen buy-in from citizens.

Implement regulatory sandboxes for innovators to test and refine their solutions.

This exercise demonstrated the need for regulatory sandboxes in the digital ecosystem to foster innovation, inform policy and regulation, enhance data protection, and promote local content and investment. In addition, a regulatory sandbox involving all the key regulators in the digital ecosystem could provide innovators with a holistic approach to compliance, which could provide ease to innovators to be able to engage with all regulators through one process.

Create incentives for early stage-compliance.

Incentives for early-stage compliance can encourage innovators to prioritize data protection from the start, fostering the understanding that data protection is innate to—rather than a hindrance of—effective digital innovation. With these incentives in place, which may include elements such as targeted government support, explanatory toolkits and templates, and funding opportunities, innovators are more likely to produce secure, privacy-preserving digital solutions—which, in turn, increases government uptake and encourages further innovation.

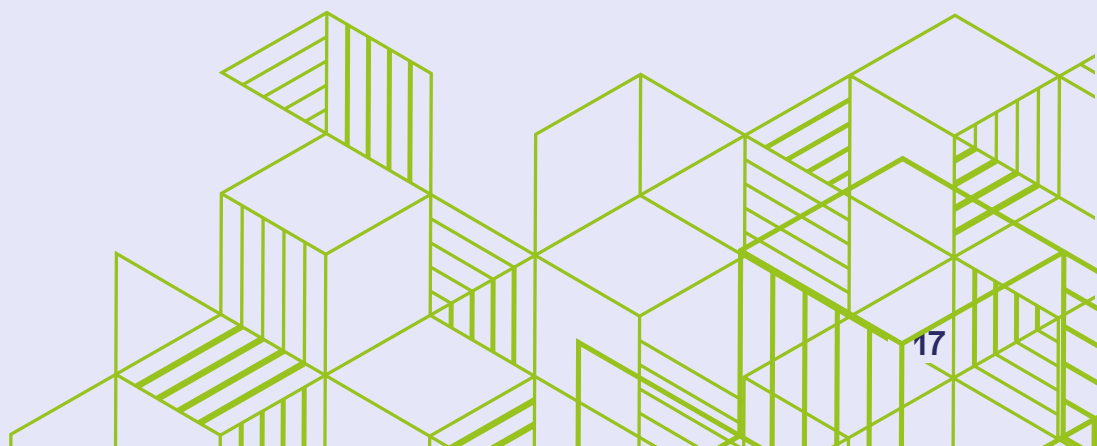
Invest in capacity building across the innovation and startup ecosystem.

This exercise highlighted the need for capacity building for innovators and the start-up ecosystem. With many start-ups facing common constraints, clear barriers in technical knowledge, policy and governance expertise, and ecosystem support emerge. To better advance both data protection principles and trusted innovation, capacity-strengthening opportunities, including training programs, partnerships with universities and academic institutions, and scholarships within the tech sector are needed.

Foster a Whole-of-Government approach to data protection.

To build lasting trust and consistency, data protection needs to be promoted across all aspects of government. As DPI is set to underpin most digital citizen services across multiple sectors and departments, and as AI becomes more embedded in public service delivery, data protection must guide how these systems are conceived, built, and used. Embedding privacy-by-design principles into the daily processes and systems of public institutions can create shared ownership and stronger accountability. When other agencies work hand-in-hand with data protection authorities, it helps make data protection a routine part of technology and governance design, driving a mindset and culture of trust across government.

For instance, governments could make data protection compliance a core step in all IT clearance and digital-service approvals. Before launching any new platform, the regulatory Ministry, Department or Agency would complete a DPIA and obtain clearance from the data protection authority confirming adherence to privacy-by-design principles. Embedding this within existing approval workflows, like procurement or security reviews, would institutionalize data protection as a default feature of government technology projects.



Conclusion

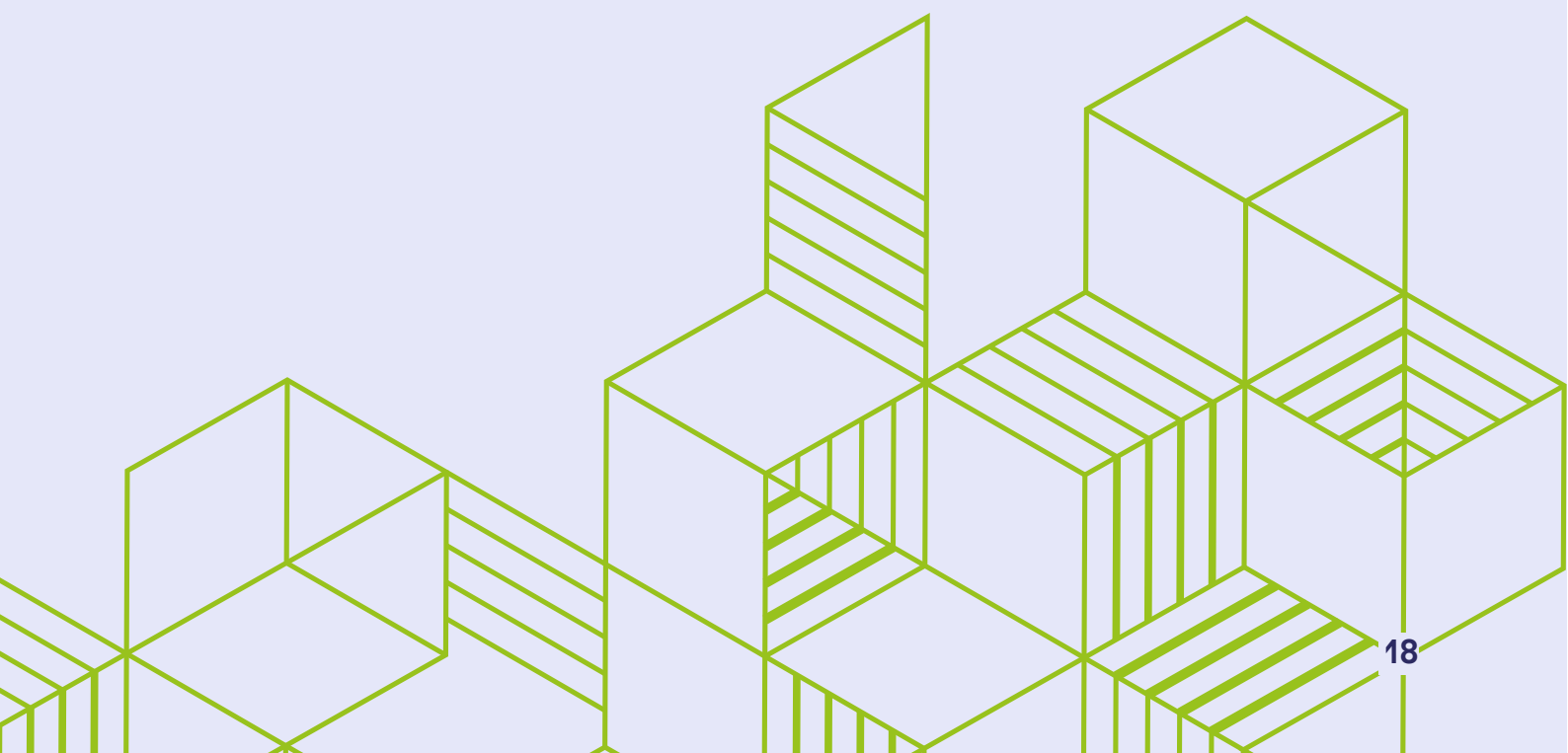
As Nigeria strengthens its approach to digital public infrastructure (DPI) and AI-powered solutions continue to advance, the combined potential to drive transformative benefits is immense—from more efficient government service delivery to greater inclusion and sustainable economic development. Yet, to ensure that these digital tools and systems are trustworthy, reliable and secure, robust data protection measures are crucial. Effective data policy and regulation can spur responsible innovation while also helping ensure the rights, privacy, and interests of people and communities are protected.

Because the innovation ecosystem is central to Nigeria's digital transformation journey, local innovators and start-ups play a key role in integrating and promoting effective data governance. Yet, common barriers can hinder their participation, as funding, capacity, and technical constraints make adhering to such regulations a challenge.

NDPC has illustrated its dedication to overcoming these barriers by promoting effective, trusted data protection and governance. This collaborative effort between NDPC and DIAL demonstrates the value of regulators adopting a hands-on approach to both institutionalizing and advancing good practices.

By working alongside implementors, NDPC and DIAL were able to better understand and provide solutions to the core challenges the innovators faced, as well as embed safeguards throughout the design process.

This work sets the foundation for future digital innovations, which, when combined with an understanding of data protection best practices, can both address pressing needs and promote an effective, trusted data ecosystem for people and communities across the country.



Endnotes

1. Digital Public Infrastructure and Development: A World Bank Group Approach. The World Bank. March 2025. <https://openknowledge.worldbank.org/server/api/core/bitstreams/bb08d389-cfbf-4417-9415-b9f65ef5c1f4/content>
2. “Machine translation is almost a solved problem.” The Economist. 11 Dec. 2024. <https://www.economist.com/science-and-technology/2024/12/11/machine-translation-is-almost-a-solved-problem>
3. Flinders, M., Smalley, I., & Schneider, J. “AI fraud detection in banking.” IBM. <https://www.ibm.com/think/topics/ai-fraud-detection-in-banking>.
4. Radanliev, P. “AI Ethics: Integrating Transparency, Fairness, and Privacy in AI Development.” Applied Artificial Intelligence, 39(1). 2025. <https://doi.org/10.1080/08839514.2025.2463722>
5. “Enrollment Report – Overview.” National Identity Management Commission. June 2025. <https://nimc.gov.ng/nin/enrolment-report/june-2025>
6. “NIMC Launches NIN Authentication Service (NINAuth) for Secure and Seamless Identity Authentication & Verification for all government services.” National Identity Management Commission. 6 May 2025. [https://nimc.gov.ng/press-releases/nimc-launches-nin-authentication-service-\(ninauth\)-for-secure-and-seamless-identity-authentication-&-verification-for-all-government-services](https://nimc.gov.ng/press-releases/nimc-launches-nin-authentication-service-(ninauth)-for-secure-and-seamless-identity-authentication-&-verification-for-all-government-services)
7. Nigeria Governors Forum “Nigeria - DPI Readiness of States - The Digital Public Infrastructure (DPI) Readiness Report.” July 2025. <https://ngfrepository.org.ng:8443/handle/123456789/7103>
8. “The African AI Ecosystem Top 20 Countries.” AI Expo Africa. 29 Aug. 2025. <https://aiexpoafrika.com/the-african-ai-ecosystem-top-20-countries/>
9. AI in Government. OECD.AI Policy Observatory. <https://oecd.ai/en/gov/issues/overview>
10. Nigeria Data Protection Regulation 2019. National Information Technology Development Agency (NITDA). 2019. <https://nitda.gov.ng/wp-content/uploads/2020/11/NigeriaDataProtectionRegulation11.pdf>
11. Nigeria Data Protection Regulation 2019: Implementation Framework. National Information Technology Development Agency (NITDA). March 2020. <https://demo.ndpb.gov.ng/Files/ImplementationFramework.pdf>
12. Nigeria Data Protection Act, 2023. 2023. https://cert.gov.ng/ngcert/resources/Nigeria_Data_Protection_Act_2023.pdf

13. Nigeria Data Protection Act, 2023, General Application and Implementation Directive (GAID) 2025. Nigeria Data Protection Commission (NDPC). January 2025. <https://ndpc.gov.ng/wp-content/uploads/2025/07/NDP-ACT-GAID-2025-MARCH-20TH.pdf>

Acknowledgements

This paper was co-authored by the Digital Impact Alliance (DIAL) and the Nigeria Data Protection Commission (NDPC).

We gratefully acknowledge the valued contributions of Dr. Vincent Olatunji CPPPS, CDPO, FIIM - The National Commissioner/Chief Executive Officer, Babatunde Bamigboye Esq. CDPRP - Head, Legal, Enforcement and Regulations Department and Ibukunoluwa Owa Esq. CIPP/E - Head, Regulations Unit in shaping the development of this paper. We also extend our thanks to DIAL team members – Adeola Bojuwoye, Diana Sang, Talla Ndiaye, Trev Harmon, Abby Garmon, and Siane Monreal – for their thoughtful input and support throughout the process.

© Copyright 2025, Digital Impact Alliance (DIAL) and the Nigeria Data Protection Commission (NDPC).



digital
impact
alliance