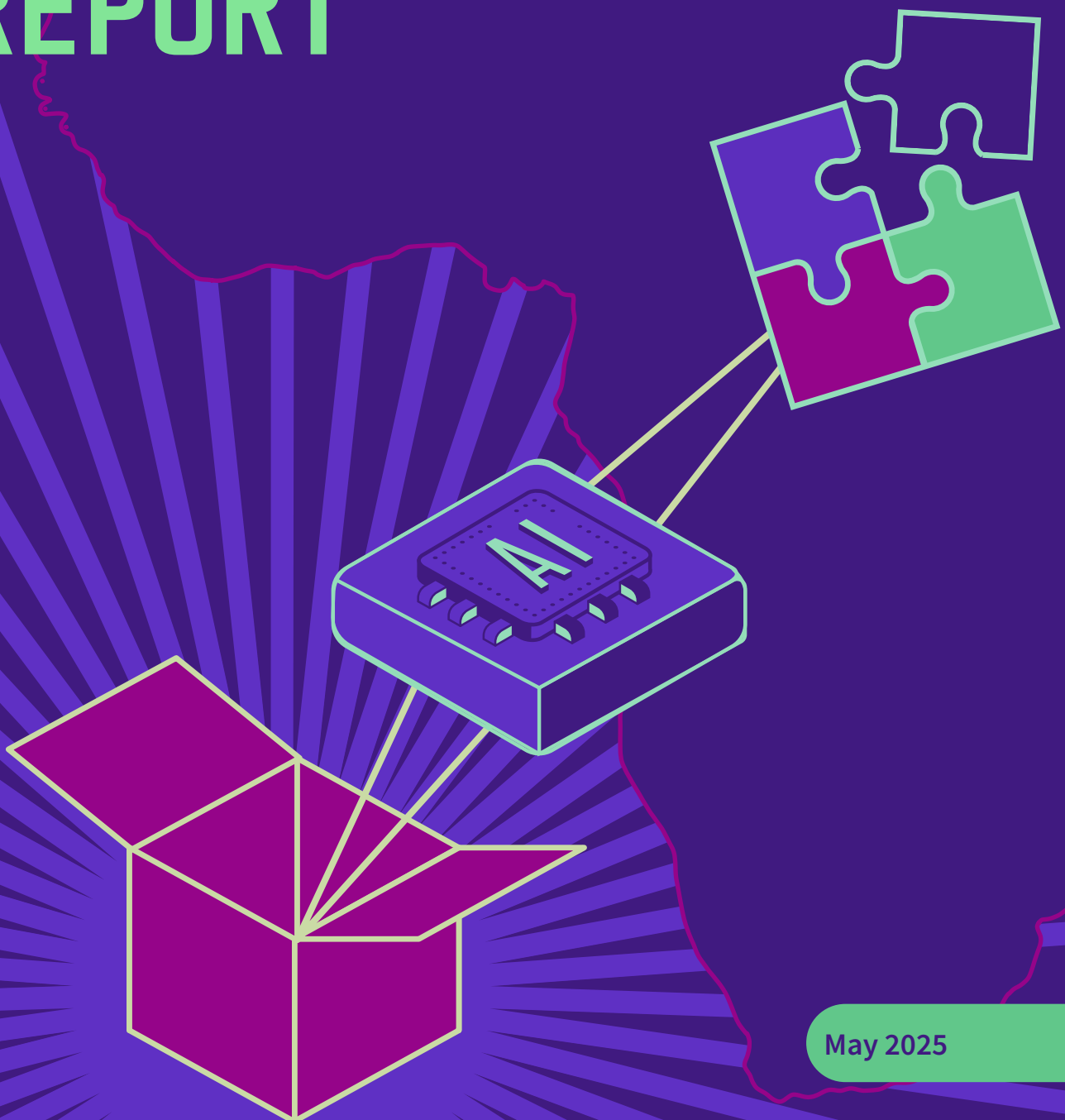
DATASPHERE INITIATIVE

ABUJA-NIGERIA AI SANDBOXES CO-CREATION LAB REPORT



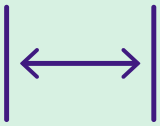
May 2025

Acknowledgements

This Co-creation Lab Report is authored by **Morine Amutorine**, Africa Sandboxes Forum Lead, and **Risper Onyango**, Research Assistant, Datasphere Initiative. The Datasphere Initiative would like to thank all of the participants who contributed their time, insights, and expertise to this co-creation lab. This workshop was enriched by the valuable perspectives of a diverse group of stakeholders from across the digital policy and data governance ecosystem.

Our gratitude goes to **Dr. Jimson Olufuye**, Principal Consultant Kontemporary Konsulting Ltd, **Timmy Ambali**, C.O.O Kontemporary Konsulting, **Adaobi Nwankwo**, Deputy Manager Nigeria Data Protection Commission, **Adam Odufuye**, Manager Dot-Engee Nigeria Enterprises, **Kayode Oyeyemi**, Snr. Programme Officer AfICTA - Africa ICT Alliance, **Oluwasegun Omolosho**, Program Officer AfICTA - Africa ICT Alliance, **Timmy Agboola**, Technical Assistant Nigeria Data Protection Commission, **Ismaila Lamidi**, Snr. Software Engineer Kontemporary Konsulting, **Ifeoluwa Olufuye**, Corporate Affairs Manager Kontemporary Konsulting, **Miqdad Sanda**, Officer 1 Nigeria Data Protection Commission, **Ijeoma Olorunfemi**, Principal Correspondent News Agency of Nigeria, **Oluwatosin Ogunleye**, Technical Assistant Nigeria Data Protection Commission, **Caroline Okafor**, Technical Assistant to the National Commissioner on Legal Services Nigeria Data Protection Commission, **Adedeji Adeniran**, Director CSEA, **Chukwuka Onyekwena**, Executive Director CSEA, **Adeola Bojuwoye**, Manager Nigeria Digital Impact Alliance, **Jesudunni Olufuye**, Intern Kontemporary Konsulting, **Bashir Abdulraheem**, Team Member Nest Africa AI Innovation Lab, **Eriba Williams**, Digital Forensics Examiner Eriba Digitalfootprints Nig. Ltd, **Blossom Idigbo**, Digital Forensic Examiner 1 Digital Footprints Nig. Ltd, **Ona Oshen**, Executive Director Responsible AI Africa, **Collins Nnabugwu**, Chief Executive Officer Cyber Future Academy CFA, **Olaniyan Taiwo**, Head Data Center Office of the Auditor-General for the Federation, **Oluwafemi Owoeye**, Technical Assistant NDPC, **Tolulope Ibitoye**, Technical Assistant NDPC, **Babagana Digima**, Deputy Director New Media & Information Security Nigerian Communications Commission, **Sadiq Ahmed**, Deputy Manager Nigerian Communications Commission (NCC), **Inye Kemaborika**, Partner TLDS Consulting, **Salim Ibrahim**, Innovation Unit NDPC, **Bayo M. Onimode**, NCS, and **Rex Abidogun**, CEO Management Edge Ltd.

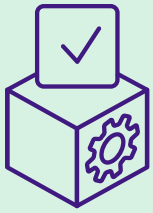
KEY INSIGHTS



While sandbox methodology is gaining traction in Africa, **understanding and awareness gaps remain**. Sandboxes are often mistaken for technical pilots or traditional consultations. This signals the need for hands-on, context-specific capacity-building that demystifies the "what, how, and where" of sandboxing.

Data Protection Authorities are emerging as pivotal to advancing responsible innovation, best positioned to guide AI and cross-border data sandboxes while ensuring alignment with data protection laws and fostering public trust.

Data Protection Authority - led sandbox models provided practical inspiration. International examples like Bermuda's PINK Sandbox, Brazil's AI/Data Protection Sandbox, and Singapore's PETs Sandbox demonstrate how DPAs can lead safe, inclusive experimentation, demonstrating a clear path of serving as enablers, not just enforcers, of ethical innovation.



Responsible sandboxing requires deliberate, inclusive design, with intentional tools for participatory digital governance, featuring clear governance guardrails, early stakeholder engagement, public trust mechanisms, and shared evaluation frameworks from the outset.

TABLE OF CONTENTS

INTRODUCTION

As Africa makes strides towards a Single Digital Market, the urgency for harmonized cross-border regulation and responsible AI governance continues to grow. Seamless cross-border data flows are key to unlocking the continent's potential in trade, development, and digital innovation. The rapid adoption of emerging technologies, coupled with the growing adoption of agile data governance such as regulatory sandboxes, offers a unique and timely opportunity to shape a harmonized, forward-looking digital economy. This was the motivation for our 2nd AI Sandboxes Co-creation Lab held in Abuja around the Network of African Data Protection Authorities (NADPA) Conference.

> ***Our Sandbox co-creation labs are spaces for stakeholders to collaboratively frame and design responsible sandbox models.***

With a good blend of participants, the lab attracted representation from diverse practitioners from government, civil society, private sector, innovators, and start-ups. A notable dialogue with key regulators from the Nigeria Data Protection Commission (NDPC) and Nigeria Communications Commission (NCC), key players in the Nigerian data ecosystem, confirmed the timely need for sandboxes. This is not only for addressing the challenges they are navigating but also for advancing efforts towards the ambitions they harbor, such as aligning regulatory frameworks with international standards and regional integration, among other things.

Participants were at varying levels of understanding of sandboxes, which made the discussion rich, ranging from defining basic terminology and sharing examples of relevant sandbox use cases, to an engaging design lab where participants designed sandboxes for high-impact cases where sandboxes could make a difference.

The high level of active participation and enthusiasm displayed by individuals – through their engagement with presenters, reactions to interactive activities, and team collaboration – underscored stakeholders' interest in the practical design and development of sandboxes.

Our objectives were clear: to explore the evolving role of sandboxes in advancing data protection and innovation; to understand how regulatory sandboxes can support responsible AI adoption and enable data-driven innovation across borders; and to identify opportunities, challenges, and pathways to enabling cross-border regulatory collaboration.

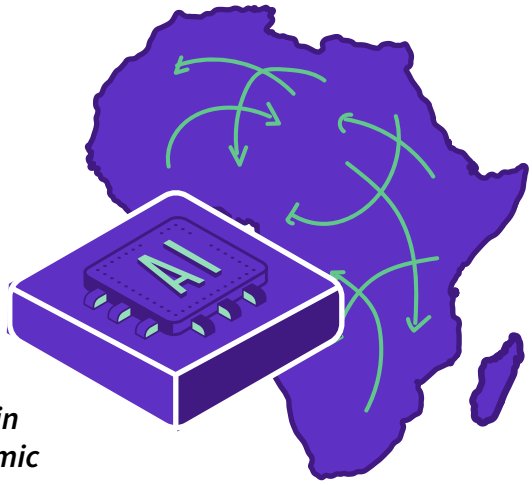
This lab is another step in our work towards catalyzing a regional approach to responsible AI experimentation, promoting policy harmonization, and deepening multi-stakeholder engagement in the governance of emerging technologies. Below we present outcomes and lessons from the co-creation lab activities.

Reflections from Mr Babagana Digima, Head - New Media and Information Security, Nigeria Communication Commission (NCC)

The discussion on sandboxes and artificial intelligence is truly a timely and strategic intellectual engagement, and from the perspective of the NCC, as a regulator of the communication sector, we recognize AI's immense potential to be transformative, improving service delivery by enhancing network optimization and addressing complex social and economic challenges. We also recognize the regulatory uncertainties and questions ranging from building for privacy and data protection to bias, transparency, accountability, and cybersecurity.

It's clear that **tools like sandboxes provide an enabling environment for collaborative learning and foster an evidence-based approach to policymaking**. This aligns perfectly with the NCC's commitment to actively explore adaptive regulatory models that can keep pace with technological advancements and guide innovation responsibly.''

AFRICA SANDBOXES FOR AI AND CROSS-BORDER INITIATIVES



> ***Sandboxes are safe spaces to test new technologies and practices against regulatory frameworks or experiment with innovative uses and means of governing data. Initially used in FinTech, sandboxes are now being applied to broader economic sectors—from transportation to telecommunications to AI. They can be operational, regulatory, or hybrid.***
> - Datasphere Initiative -

As Africa advances toward a Single Digital Market, the need for harmonized cross-border regulation and responsible governance of emerging technologies, particularly artificial intelligence, has never been more urgent. Seamless data flows across borders are central to unlocking the continent's potential in trade, financial inclusion, and innovation. In this context, regulatory sandboxes have emerged as a timely mechanism to test, learn, and iterate new approaches to technology governance in a safe, controlled environment.

To this end, our attention turned to AI and cross-border initiatives, two domains where the lack of harmonized regulation and shared testing mechanisms pose some of the most pressing and immediate risks to trust, safety, and interoperability. Exploring how regulatory and operational sandboxes can support responsible AI adoption and enable data-driven innovation across jurisdictions, the discussions in our co-creation process spotlighted the promise of AI and cross-border sandboxes to facilitate trusted data flows and scale innovation.

AI sandboxes are not one-size-fits-all. Their design, scope, and purpose can vary significantly, from compliance-focused models to innovation-driven or community-led platforms. Kenya is currently leading the way with its ICT Sandbox[1], operated by the Communications Authority of Kenya. Unlike fintech-specific sandboxes, this initiative has a broader mandate, making space for experimentation with a wide range of ICT innovations. While it has yet to test AI solutions specifically, its flexible scope positions it as a promising pioneer for AI governance on the continent.

As of January 2025, research by the Datasphere Initiative revealed that there are 66 sandboxes related to data, AI or technology worldwide.[2] Of these, only 23 countries globally are actively planning or operating AI-specific sandboxes to address emerging technological challenges and opportunities.[3] Africa currently has none. This gap in Africa points to an untapped opportunity to lead with sandbox models that center safety, accountability, and inclusion in AI development.

---

[1] CA (n.d), ICT Regulatory Sandbox, Communications Authority of Kenya.

[2] Datasphere Initiative (2025). Sandboxes for AI: Tools for a new frontier. https://www.thedatasphere.org

[3] Datasphere Initiative (2025). Sandboxes for AI: Tools for a new frontier. https://www.thedatasphere.org

Cross-border sandboxes, meanwhile, offer even greater potential. These frameworks involve collaboration between regulators in two or more jurisdictions and can act as powerful tools for regional integration. Their core purpose is to foster regulatory alignment and enable innovation that can scale across multiple markets. By offering real-time insights into how digital products operate in diverse legal and cultural environments, **cross-border sandboxes help streamline licensing, support reciprocal arrangements, and reduce duplication of regulatory efforts**. They also help reduce costs by allowing countries to test joint models at the regional level, leaving local adaptations to be tailored to national realities.

A compelling example is the Pacific Regional Regulatory Sandbox,[4] which brings together financial regulators from seven countries in a shared virtual space. This platform has enabled fintech firms to test products under joint supervision and has led to over 118 policy changes, demonstrating the tangible impact of such collaborative testing environments. In contrast, no African sandbox currently reports such concrete outcomes. Of the 25 sandboxes analyzed across Africa,[5] few provided publicly available results, underscoring a broader challenge: limited communication and documentation of sandbox learnings. This lack of transparency presents a significant barrier to knowledge sharing, institutional memory, and evidence-based policymaking.

Additionally, the ASEAN-GSMA Regulatory Pilot Space for Cross-Border Data Flows[6] demonstrates other global efforts that offer useful templates. This initiative sought to provide a safe environment where policymakers can test solutions for enabling cross-border data sharing, an approach that could serve Africa well, particularly in regions where regulatory maturity varies widely.

Our discussions revealed that to realize the full promise of sandboxes for AI and cross-border collaboration in Africa, a deliberate and strategic approach is needed: one that foregrounds local context, fosters regional collaboration, and ensures outcomes are captured, shared, and used to strengthen governance across the continent.

Reflections from Dr. Jimson Olufuye, Principal Consultant at Kontemporary Konsulting

The growing volume of cross-border data flows and the importance of developing AI systems that are both integrated and adaptable underscores the critical need for robust cross-border data sharing and interoperability. Methodologies such as sandboxes are essential for better data and product management.

There is also a need to optimize data protection processes to actively encourage cross-border data exchange and facilitate the easy scaling of products not only across West Africa but also beyond.

The diversity of AI and data protection laws across Africa, as well as the fragmentation among institutions, poses challenges. This necessitates collaboration among regulators to harmonize regulatory frameworks and achieve effective and inclusive data governance on the continent.

[4] Reserve Bank of Fiji (n.d), Pacific Regional Regulatory Sandbox Guidelines, www.rbf.gov.fj

[5] Datasphere Initiative (2025). Sandboxes for AI: Tools for a new frontier. https://www.thedatasphere.org

[6] GSMA (2019), ASEAN-GSMA Regulatory Pilot Space for Cross-Border Data Flows, www.gsma.com

THE PIVOTAL ROLE OF DATA PROTECTION AUTHORITIES IN AI AND CROSS-BORDER SANDBOXES

As countries across Africa and globally look to build trustworthy digital ecosystems, data protection authorities (DPAs) are emerging as critical anchors in the development and oversight of both AI and cross-border sandboxes. During the session, participants explored this role through real-world scenarios, global case studies, and interactive dialogue, revealing how DPAs serve not only as regulators, but as enablers of innovation, standard-setters, and public interest stewards.

Global Use Cases that reinforce the DPA's Role

Participants explored three global sandbox models that showcase the varying ways DPAs can lead or support responsible innovation:

- **Bermuda's "PINK" Sandbox**[7] (Privacy, Innovation, and Knowledge-sharing), launched in 2022, started as a capacity-building initiative under the national privacy authority and is now expanding to include co-design of products and services based on applicants' needs. Its flexible, DPA-led approach reflects how sandboxes can evolve in tandem with national privacy objectives.

- **ANPD**[8] Brazil's AI and Data Protection Sandbox, is grounded in a regulatory framework, and is explicitly designed to test the alignment between AI innovations and existing data protection legislation. The DPA's central role ensures that AI governance is not developed in a legal vacuum.

- **Singapore's Privacy Enhancing Technologies (PETs) Sandbox**[9] adds the dimension of funding and technical support to its framework. With DPA oversight, innovators are provided with grants and APIs to test privacy-focused solutions. This model emphasizes that regulatory sandboxes can incentivize innovation while maintaining oversight and public trust.

[7] PrivCom (n.d), PINK Sandbox Bermuda, www.privacy.bm

[8] Ministry of Justice and Public Security (2023), ANPD's Call for Contributions to the regulatory sandbox for artificial intelligence and data protection in Brazil is now open, www.gov.br

[9] IMDA (2022), Launch of Privacy Enhancing Technologies Sandbox, Personal Data Protection Commission Singapore

Such scenarios underscore why regulatory sandboxes are necessary to proactively address the tensions around privacy and data protection, and additionally, illustrate that when DPAs are actively involved, sandboxes are more likely to integrate rights-based safeguards from the start, promote transparency, and encourage cross-sector collaboration.

Ultimately, the session emphasized that data protection authorities are not simply regulators, but strategic enablers of safe, inclusive, and scalable innovation. Their leadership ensures that sandboxes serve public interest, respond to emerging risks, and build trust, not just between innovators and regulators, but with the broader public whose data and rights are at stake across sectors.

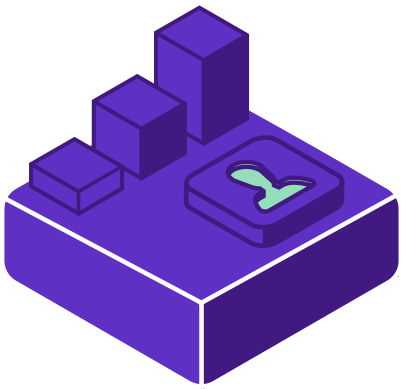
Whether the focus is on AI, cross-border data flows, or privacy-enhancing technologies, DPAs bring the legitimacy, expertise, and accountability needed to make sandboxes more than just test environments. They turn them into governance tools, spaces where policy and practice meet, where innovation is shaped with rights in mind, and where the future of digital ecosystems can be safely and collectively imagined.

Reflection from Adaobi Nwankwo, Head of Innovation Unit, Nigeria Data Protection Commission (NDPC)

Recognizing the lab as a vital step forward in shaping how we responsibly and innovatively harness artificial intelligence across the African continent, Ms. Adaobi, representing the NDPC, shared the Commission's perspective.

The NDPC is actively looking at a regulatory sandbox as **a safe and structured environment for testing data-driven solutions with real-time regulatory guidance**. Its primary goal is to test Nigeria’s data protection regulation within an environment that fully complies with national laws. This initiative aims to balance innovation with AI responsibility, ensure trustworthy datasets for AI development, and foster fair AI systems.

This co-creation is a platform for more collaboration, to share and identify practical solutions and design pathways that ensure Africa's AI future.



CHALLENGES AND LIVED EXPERIENCES OF SANDBOXES

What comes to mind when you think about sandboxes?

One participant questioned, “Is this the same as the childhood sandbox we used to play in? Is it a physical space, or something virtual?” This prompted a broader discussion on what sandboxes truly represent in digital governance. It was clarified that modern regulatory and operational sandboxes are typically virtual environments, though they may include physical components such as in-person engagement or live testing in controlled settings. The core idea is that these sandboxes allow for experimentation, particularly with new data-driven solutions, and in many cases under the supervision/with the involvement of an authority.

Participants further expressed concerns about what it means to test data-driven solutions in these environments. **If personal data is being used, even in a test setting, what safeguards exist to protect the people behind the data?** One participant asked pointedly, **“What’s to stop someone from using my data against me in the future, especially if I later disagree with the entities involved? What’s the safety guarantee for participating?”**

These concerns highlighted a deep-seated issue: trust in the institutions and actors behind sandbox testing. It was emphasized that sandboxes cannot be seen as experimental free-for-alls. There must be clearly defined rules of engagement, terms and conditions that outline how data will be collected, stored, processed, and shared. Sandbox frameworks must specify the scope of the sandbox, its boundaries, and regardless of the testing results, what happens to the data once testing ends.

A key insight from the session was that sandboxes must go beyond a closed loop of innovators and regulators; they need to meaningfully involve the people whose data or lived experiences are at stake. The Datasphere Initiative’s sandbox methodology addresses this by ensuring comprehensive stakeholder mapping and an engagement plan are built into the earliest phases, enabling true multistakeholder participation. Participants also emphasized the need for clear definitions of success and transparent criteria for when a product is ready to exit the sandbox, elements that Datasphere Initiative incorporates through its dedicated communication and engagement strategies.

Why have you not engaged in or led a sandbox before?

Participants reflected on a wide range of reasons why they had not engaged in or led sandbox initiatives, citing both structural challenges and practical barriers. Key concerns included overly burdensome documentation requirements, particularly for smaller developers with limited capacity.

Sandbox Lived Experience - Adeola Bojuwoye, Manager (Project Lead-Nigeria), The Digital Impact Alliance). *Adeola has a background in software development and shared his experience participating in a certain sandbox.*

Onboarding challenges: The process for onboarding innovators was significantly cumbersome. The user experience was not user-friendly, with lengthy and at times, unrealistic documentation requirements. This highlights **a need for regulators to have a deeper understanding of their ecosystem and the varied maturity of solutions entering the sandbox**. In our case, regulators made assumptions about innovators having established structures in place, which was often not the case.

Clarity on exit and results: There was a lack of clarity regarding outcomes. The sandbox process needs to explicitly define what constitutes a "pass" or "fail" and outline the subsequent procedures. Without this clarity, stakeholders are left to make assumptions.

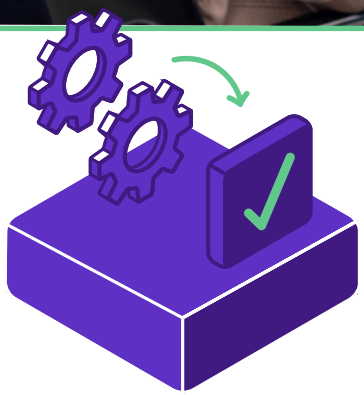
Unclear approval process: The overall approval process lacked transparency. Sandboxes should clearly articulate expected outputs and establish transparent criteria for success and completion.

Others pointed to weak incentives and unclear pathways from sandbox participation to real-world approval or policy influence, making the effort seem disconnected from tangible outcomes. While sandboxes are designed for mutual learning, with regulators gaining insights from innovators and innovators from regulators, roles and responsibilities are often not clearly defined. This lack of clarity creates a significant disconnect, leading to wasted time and resources within the sandbox environment.

Additionally, the absence of sustained political will and policy continuity was seen as undermining long-term impact, especially in environments where sandboxes risk being treated as temporary projects rather than foundational governance tools.

What challenge would you address if given the opportunity to run a sandbox?

When asked what challenge they would address if given the opportunity to run a sandbox, participants' responses pointed to a range of unresolved issues: controlling who processes their data, ensuring meaningful consent, managing data across its full lifecycle, and reconciling data sovereignty with the benefits of cross-border data flows. Additionally, they raised the need for transparency, cybersecurity, and user understanding in data processing, especially when AI or automated decision-making is involved.



RESPONSIBLE SANDBOXING

Participants teamed up to brainstorm and pinpoint challenges and opportunities where AI and crossborder sandboxes could drive meaningful change.

Three distinct sandbox concepts were developed;

1. Africa Universal Cross-Border Sandbox (AUCS)

For a cross border sandbox, one group explored ensuring software systems are universally acceptable. The challenge: the absence of standardized programming languages, documentation, and localized interfaces results in software functioning well in one country and failing or becoming unusable in another. The **Africa Universal Cross-Border Sandbox (AUCS)** is an example of a proposed regulatory framework to tackle interoperability challenges caused by machine language barriers, aiming to ensure that software systems are universally acceptable across jurisdictions. This sandbox underscored the importance of technical compatibility as a foundation for trusted data flows and cross-border digital trade. Details of this sandbox are covered under annex 1.

2. AI for Good Sandbox

Meanwhile, two teams addressed responsible AI governance. The first, **AI for Good Sandbox**, envisioned a hybrid model to foster awareness and ethical literacy around AI use in Nigeria. The team envisioned a sandbox design that emphasized the need for national alignment with legal frameworks like the Nigeria Data Protection Act and National AI Strategy, and highlighted risks such as false compliance and the disconnect between global ethical norms and local realities.

3. Naija LLM Sandbox

The second, **Naija LLM Sandbox**, focused on creating a culturally grounded and linguistically inclusive AI large language model built by and for Nigerians. The sandbox framework brainstorm aims to address challenges like inconsistent policy support, limited technical capacity, and the threat of bias and profiling in AI models. Both sandbox discussion details are detailed in the annexes.

The sandboxing activity, while constrained by time limitations and participants' varying levels of sandbox familiarity, nevertheless demonstrated the value that sandboxes (regulatory or operational) can provide. The exercise helped narrow down specific use cases (drawn from the challenges and opportunities previously discussed) that would yield the greatest sandbox impact. It also identified key stakeholders that participants deemed essential for running and participating in these sandboxes. Most importantly, the activity reinforced the recognition that sandboxes can serve as effective mechanisms for ethical, inclusive, and context-sensitive governance of emerging technologies across Africa.

Responsibility elements

Each of the discussions reinforced that responsible sandboxing requires more than just a testing environment, it demands clear governance guardrails, early and continuous stakeholder inclusion, and built-in accountability mechanisms.

Participants strongly aligned with the idea that both AI and cross-border sandboxes must be designed with responsibility at their core, ensuring they work across diverse stakeholder groups and real-world contexts. Through prompts on cultural and technical factors such as trust barriers, incentive structures, required skill sets, data risks, and interoperability challenges, the dialogue surfaced core principles that emerged as foundational to responsible sandbox design:

- Clarity and transparency in how the sandbox operates, including entry and exit criteria, decision-making processes, and data use rules.

- Co-creation and cross-pollination across stakeholder groups, ensuring that sandboxes reflect multiple perspectives, from regulators and developers to end-users and impacted communities.

- The presence of interdisciplinary technical support and expert skills - Both AI and cross-border sandboxes require not only technical know-how but also legal, ethical, linguistic, and socio-political insight, particularly at the design stage. Without this, sandboxes risk being built with blind spots that exclude or misrepresent key user groups. In the case of AI, this may lead to systems that fail to recognize local dialects or encode harmful biases. In cross-border contexts, it can result in platforms that cannot scale across jurisdictions or that collapse under conflicting national laws.

CONCLUSION: INCLUSION, CLARITY, ACCOUNTABILITY

The AI Sandboxes Co-creation Lab in Abuja surfaced a powerful convergence of urgency, opportunity, and innovation. Africa's need for trusted governance mechanisms that can keep pace with emerging technologies, particularly AI and cross-border initiatives, is more critical than ever, and sandboxes offer a vital pathway to address this need.

Across all three sandbox concepts designed during the lab, from cross-border interoperability to ethical AI awareness and locally trained large language models, the common thread was the recognition that sandboxes must be rooted in **inclusion, clarity, and accountability**. Additionally, participants emphasized the need for sandboxes to be purpose-built for Africa's realities; serving as responsive mechanisms shaped by our local contexts, regulatory environments, and societal needs.

The lab represented a step toward a new practice. It underscored the need to embed responsibility from design to deployment, to involve citizens and regulators as co-creators, and to treat sandboxing as a cornerstone of agile governance in Africa's digital transformation.

Reflections from Sophie Tomlinson, Director of Programs, Datasphere Initiative

In the age of AI, and during what some call the "data century," it is clear that all countries are facing the same challenge: How to responsibly unlock the value of data and the digital economy for all. Supporting governments, businesses, civil society, and academia in this important and complex task is what the Datasphere Initiative is all about.

The Africa Sandboxes Forum aims to support the growing use of sandboxes across the African continent and foster cross-border collaboration. It provides research insights on how sandboxes are being used across countries; facilitates interactive workshops, such as this lab, to bring stakeholders together to design and co-create sandbox possibilities for emerging tech challenges; and also offers training and personalized coaching to assist organizations in sandbox design and implementation. Sandboxes serve as vital tools to develop agile and fit-for-purpose regulation and responsible technological innovation.

These co-creation labs are an opportunity for practitioners to step into a sandbox journey, exploring what sandboxes are and their potential for addressing complex challenges around data protection and privacy, AI, and cross-border data flows. Ultimately, this complexity is not only about the rules governing data's use but also about the global, regional, cross-sectoral, and cross-stakeholder relationships that shape how data is shared, protected, and leveraged to help us deal with local and global challenges.

ANNEXES

Annex I: Sandbox proposals from the design lab

1. A cross border sandbox for ensuring software systems are universally acceptable

Proposed name: Africa Universal Cross-border Sandbox (AUCS)
Sandbox Type: Regulatory
Challenge: Machine Language Barriers. Presently, the absence of standardized programming languages, documentation, and localized interfaces results in software functioning well in one country and failing or becoming unusable in another.
Goal: To ensure software systems are universally acceptable
Stakeholder to involve: ICANN, Academia, Data Protection Authorities
Regulatory Status: None

In light of Africa striving for greater digital integration, where cross-border trade is the cornerstone of economic transformation, a fundamental question emerging is whether our systems can speak to one another. This gave rise to the idea of the **African Universal Acceptance Cross-Border Sandbox (AUCBS)**, to test and validate whether software systems across African countries are "universally acceptable" in both design and implementation. The sandbox proposed the idea that each system entering the sandbox must be Universal Acceptance (UA) ready; meaning it can handle diverse languages, scripts, formats, and regulatory parameters.

The promise of AUCBS is if our systems can talk to each other, our people and economies can too. The initiative argued that universal acceptance and technical compatibility are prerequisites for digital trade, cross-border services, and regional economic growth. The incentives highlighted included interoperable systems that enable collaboration, validated compatibility which fosters mutual trust, and reducing technical and legal friction to open up the African market.

The goal of the sandbox was to create a technical and policy testing environment where digital solutions can be evaluated for interoperability, legal adaptability, and inclusive access, by addressing the systems language barrier challenge that hinders all software systems from speaking a universally acceptable programming language, and thus being synchronised across countries. AUCBS is about enabling digital infrastructure to cross borders without breaking laws, excluding users, or undermining trust. However, these benefits come with real risks. Data sovereignty remains a pressing concern: who controls the data as it moves between systems, and how do we prevent a "universal" framework from becoming a single point of failure, whether technically, politically, or economically? Participants also cautioned against overlooking language and local context, noting that universal acceptance too often defaults to external standards that may not reflect Africa's diverse digital realities.

The responsibility within the sandbox is shared: Governments bring legal and institutional knowledge. CSOs raise the voice of communities and marginalized users. Developers test their tools against cross-border expectations. Academia contributes research and evaluation. The private sector provides

use cases and innovation. Key stakeholders proposed included ICANN, regional Data Protection Authorities (DPAs), NIRA, National Communications Commissions, ISOC, academia, the African Union Commission, ITU, and the UN.

Success wouldn't just be systems passing technical tests, but would also include the emergence of mutual trust across borders, underpinning shared understanding, transparent rules, and a culture of accountability. It is not only about lawmaking, but about standard-setting.

2. A Sandbox for creating awareness and literacy for the ethical use of AI in Nigeria

Name: AI for Good Sandbox
Sandbox Type: Hybrid
Challenge: Lack of awareness around how to adopt ethical use of AI in Nigeria.
Goal: To create awareness and literacy for the ethical use of AI in Nigeria.
Stakeholders to involve: Nigeria Data Protection Commission (NDPC), NITDA, Academia, National Assembly, Federal Ministry of Communication, Innovation and Digital Economy (FMCIDE) and National Orientation Agency**.**
Regulatory Status: The Data Protection Act, Nigeria's National AI Strategy.

The AI for Good Sandbox in Nigeria was designed as a proactive step toward embedding ethical principles into the country's fast-evolving AI landscape. With a focus on raising public and institutional awareness, the sandbox aims to build literacy around the responsible use of artificial intelligence by creating a controlled environment where AI applications can be tested against existing national frameworks; namely, the Nigeria Data Protection Act and the National AI Strategy.

Stakeholders such as the Nigeria Data Protection Commission (NDPC), NITDA, the National Assembly, academia, and the National Orientation Agency (NOA) are envisioned as key contributors to this ecosystem, bringing policy, technical, and societal perspectives to the table.

The sandbox makes the case for ethical literacy, not just a policy aspiration but a functional requirement for the sustainable adoption of AI technologies. It encourages shared responsibility across sectors while enabling innovators to understand how their models align with Nigeria's legal and ethical standards. Some of the challenges highlighted were: the risk of false compliance, where systems appear to pass ethical checks without truly embodying the spirit of responsible AI, and concern about who defines ethical use, especially in a context where global norms may not always align with local realities. Furthermore, limited technical understanding among lawmakers and fragmented regulatory coordination could slow progress or create conflicting interpretations of what "ethical AI" means in practice.

Success for the AI for Good Sandbox would not only mean AI systems that are technically compliant, but a culture of informed adoption, where policymakers, developers, and everyday Nigerians understand both the promise and the consequences of AI use, ultimately contributing to a trustworthy, people-centered AI ecosystem.

3. Sandbox to create an AI LLM that speaks and listens to Nigerians, by Nigerians for Nigerians

Name: Naija LLM Sandbox
Sandbox Type: Hybrid
Challenge: Dealing with standardization, compliance, awareness
Goal: To create an AI LLM that speaks and listens to Nigerians, by Nigerians for Nigerians.
Stakeholders to involve: Private sector, Government, Telecommunication companies, National Orientation Agency,
Regulatory Status: The Data Protection Act, Nigeria's National AI Strategy.

The **"Naija LLM Sandbox"** is a hybrid regulatory and operational space designed to tackle one of the most pressing challenges in Nigeria's AI journey: developing a large language model (LLM) that truly understands and serves Nigerians, built by Nigerians, for Nigerians. Framed around the goals of localization, accuracy, and inclusion, the sandbox seeks to create an ecosystem where AI development aligns with national priorities and societal values. Drawing from the Data Protection Act and the National AI Strategy, the sandbox will serve as both a compliance testing ground and a platform to raise awareness and build capacity in AI governance. Stakeholders from across the private sector, telecommunications, government, and the National Orientation Agency (NOA) are expected to collaborate to ensure that the model is technically robust, culturally grounded, and accessible to a linguistically diverse population.

The sandbox confronts core issues such as the lack of standardized practices, inconsistent government policies, and the brain drain of AI talent, all of which undermine long-term continuity. It also aims to address the low levels of technical capacity in public institutions, which often results in missed opportunities to shape AI development in a way that reflects local needs. A major part of the challenge lies in poor localization of language and data, leading to models that misinterpret Nigerian dialects, ignore cultural nuance, or reinforce stereotypes.

Risks within the sandbox are multifaceted, such as concerns around bias, discrimination, and profiling, especially if training data does not reflect Nigeria's diversity. Security risks, including model breaches and misuse of AI outputs, pose real threats in an increasingly digitized society. And critically, the lack of consistent political will, sustained funding, and cross-sector collaboration could stall progress before tangible outcomes are realized.

Yet if successful, the Naija LLM Sandbox could lay the groundwork for a nationally relevant, linguistically inclusive, and ethically sound AI model; one that helps Nigerians engage with digital systems in their own voice, on their own terms. Success would mean more than just accuracy in language processing; it would represent a collective achievement in innovation, accountability, and national self-determination in the age of AI.

Annex II: About the co creation lab

Schedule

Africa Sandboxes for AI Co-Creation Lab - Abuja Edition
Date: 9th May 2025, Time: 8:00 am - 1:00 pm WAT
Venue: Shehu Musa Yar'Adua Centre

Time	Session
8:00 - 9:00 am	Welcome! Collection of Name Tags
9:00 - 9:30 am	National Anthem of Nigeria Opening Remarks • Datasphere Initiative • Kontemporary Konsulting • Nigerian Communications Commission • Nigeria Data Protection Commission (NDPC)
9:30 - 10:00 am	*Group Photo/Tea Break*
10:00 - 10:40 am *Session One*	**What are Sandboxes and Why do they matter for Data Protection and Privacy?** • Overview of sandbox models and their role in advancing data protection • Q&A • Roundtable Discussion (Perspectives from different stakeholder types)
10:40 - 11:20 am *Session Two*	**Sandboxes for AI and Cross border Initiatives** • Insights from Sandboxes for AI and Sandboxes for Data: creating spaces for agile solutions across borders Reports • Q&A • Introduction to sandboxing lab
11:20 - 12: 50 pm *Session Three*	**Design Lab - Responsible Sandboxing [Cross-border Sandbox |or| AI Sandbox]** 1. Framing high impact case studies - 25 min **Rapid Fire Session** 2. Designing a sandbox canvas - 35 min 3. Defining essential elements for responsible design, development, implementation and assessment of sandboxes - 15 min **Presentations - 15 min**
12:50 - 1:00 pm	• Africa Sandboxes Forum Activities & Conclusion - Datasphere Initiative • Feedback
1:00 pm - 2:00 pm	*Lunch / End of Programme*

Annex III: Still puzzled about what sandboxes are? Let's clear it up!

What would an operational sandbox look like?	*What would a regulatory sandbox look like?*
Take, for example, a situation where a developer wants to launch new software that must run across different operating systems; Windows, Linux, and macOS. Instead of releasing the software directly to the public, where users would download it onto their personal devices, encounter bugs, and send feedback, the sandbox provides a dedicated environment to test it first. Within this virtual space, the software can be installed and run across all intended systems. Developers and regulators can observe how it behaves on each platform, identify compatibility issues, performance gaps, or potential risks, and make adjustments in a controlled, non-public setting. This process ensures that by the time the software is officially released, it has already been refined to meet key standards of safety, reliability, and functionality, without exposing real users to harm. That is the essence of an operational sandbox: it enables experimentation, learning, and iteration without compromising public trust or infrastructure.	Think about mobile money. When you send money, the recipient's name pops up, because the app is interacting with a database that already holds your personal data, collected by the telecom provider when you registered. Now imagine someone wants to build a new feature on top of that system. In a regulatory sandbox, they'd be allowed to test that feature in a controlled environment, using real or simulated data, while regulators, developers, and other stakeholders, working together, check if the innovation aligns with existing rules/laws/policies, identifying any gaps, and adjusting the design to the regulation accordingly. It's a safe space to experiment, learn, and make sure innovation happens responsibly.

thedatasphere.org