LawDigits
Education | Research | Innovation

A Tech-Law Webinar

Balancing Innovation & Sovereignty;

The Nigerian Legal Framework on Cross-Border Data Transfers in the context of the global digital economy

Olamiji Ogun
Legal Consultant

Adamma Isamade
Data Privacy Professional

Mus'ab Awwal Mu'az
Digital Rights Lawyer

13 August,2025

03:00 pm - 05:00 pm

Online

https://forms.gle/UR2UQVEAc2wdLBBh8

WEBINAR SUMMARY

Title: **Balancing Innovation and Sovereignty: The Nigerian Legal Framework on Cross-Border Data Transfers in the Global Digital Economy**

Date: 13th of August 2025

Speakers: Olamiji Ogun (Legal Consultant); Adanma Isamade (Data Privacy Professional); Mus'ab Awwal Mu'az (Digital Rights Lawyer)

Moderator: Maureen Itah, Equibridge Attorneys.

Format: Expert panel discussion

Audience: Legal practitioners, privacy professionals, technology experts

thelawdigits@gmail.com

www.ebafirm.com

Overview

The LawDigits team organised a webinar which explored Nigeria's approach to cross-border data transfers. The webinar brought together legal practitioners, data privacy professionals, policymakers, and technology experts to examine how Nigeria can facilitate free data flows that fuel innovation while safeguarding its sovereignty and protecting citizens' privacy. The conversation traced the historical roots of data exchange, explored the evolution of Nigeria's regulatory response, and dissected the latest legal framework under the Nigerian Data Protection Act (NDPA) 2023. It further considered the practical challenges of enforcement, international collaboration, and global standards, highlighting the delicate balance between sovereignty and integration into the digital economy.

Introduction

Maureen Itah welcomed everyone to the maiden edition of the Law Digit Webinar series sponsored by Equibridge Attorneys (EBA). She emphasised the importance of the webinar topic in the present digital era, especially against the backdrop of the recent fine imposed by the Nigeria Data Protection Commission (NDPC) on MultiChoice Nigeria, the parent company of DStv and GOtv, of the sum of N766.24 million for violating the privacy of subscribers by sharing their data across international borders without compliance with the provisions of the NDPA.

Maureen explained the structure of the programme starting from the speaking sessions to the questions and answer session and introduced the speakers.

Key Themes and Insights

The first speaker, Mr Olamiji Ogun, explained that the idea of cross-border data transfer is not new. In pre-digital times, African societies, including Nigeria, relied on oral traditions, trade agreements, and town criers to exchange information across communities. During the colonial era, this evolved into formal systems of communication such as written records, telegrams, and telephones, which connected colonies with their colonial powers.

The real transformation, however, occurred in the late 20th century with the rise of the internet. By the 1990s, real-time global data flows became possible, eliminating geographical barriers and allowing businesses to process and store data on servers located anywhere in the world. For Nigeria, this digital revolution presented new opportunities in commerce, healthcare, finance, and education. At the same time, it raised profound questions about control, security, and accountability for personal data once it left the country's borders.

Nigeria first responded with the Nigerian Data Protection Regulation (NDPR) in 2019, a precursor to the more comprehensive Nigeria Data Protection Act, 2023 (NDPA). The Act now serves as the principal law regulating the processing of personal data.

The NDPA represents a significant leap in Nigeria's data governance. Sections 41–43 set out strict requirements for any transfer of Nigerian citizens' data outside national borders. At its core, the law recognises that data is both an economic asset and a matter of national sovereignty.

He mentioned that the first requirement of the act to perpetrate cross-border transfer is the adequacy test. Thus, before personal data can be transferred abroad, the Nigerian Data Protection Commission (NDPC) must evaluate whether the recipient country provides a level of protection essentially equivalent to Nigeria's standards. This involves assessing the destination country's legal framework, independent oversight mechanisms, remedies for breaches, and overall privacy culture. Where adequacy is confirmed, data can move without additional barriers.

Where adequacy is absent, the Act provides for appropriate safeguards, which are Standard Contractual Clauses (SCCs), i.e., pre-approved legal contracts binding both exporter and importer to data protection obligations; Binding Corporate Rules (BCRs), which are privacy policies used by multinationals to ensure consistent standards across global operations; and Codes of Conduct and Certification Schemes which are industry-led mechanisms that can supplement legal protections.

The discussion then turned to international practices and trends that Nigeria must contend with. Four dominant themes emerged:

- Data Localisation: Many countries now require sensitive categories of data to be stored domestically. Examples include Russia's stringent personal data rules and India's mandate for local storage of payment data. Nigeria itself has long required government data to be stored locally under its local content guidelines. While localisation strengthens sovereignty, it also imposes cost and infrastructure burdens on businesses.
- Privacy-Enhancing Technologies (PETs): New tools such as differential privacy and secure multi-party computation allow organisations to analyse or share datasets without revealing individual identities. These are increasingly used in finance and healthcare to reconcile the need for innovation with the duty of confidentiality.
- Harmonisation of Frameworks: Divergent national laws create compliance burdens for global businesses. Initiatives like the OECD Privacy Guidelines and the Cross-Border Privacy Rules Forum aim to harmonise standards and create interoperability. Nigeria, through the NDPA, is seeking alignment with such global norms to remain competitive and avoid regulatory isolation.
- Digital Trade Agreements: Recent trade treaties now include data flow clauses that regulate cross-border information transfers. Agreements like the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) attempt to reconcile free flows with privacy protections, often pushing back against rigid localisation rules. For Nigeria, future trade agreements may adopt similar provisions.

The NDPA 2023 and Cross-Border Data Transfers

The second speaker Mr. Mus'ab Awwal Mu'az, explained that a resilient data security regime, capable of attracting serious investments, hinges on a balanced collaboration between government leadership and private-sector engagement, anchored by clear standards, stringent enforcement, and phased implementation. Data protection must be reframed as a strategic national asset, not merely a regulatory obligation, crucial to security, growth, and digital trust.

First, awareness and education are foundational. All stakeholders, government agencies such as NITDA, NDPC, and the Ministry of Innovation and Digital Creativity, as well as private enterprises, must internalise that data sovereignty safeguards critical infrastructure, national security, and economic vitality. Elevating data protection from a mere compliance checkbox to a strategic objective creates a favourable investment climate.

Second, capital investment is indispensable. Building secure data ecosystems is capital-intensive, requiring sustained funding for hardware, software, talent, and continuous modernisation. The government should explicitly prioritise and allocate resources for secure data infrastructure while enabling private capital through incentives, tax relief, guarantees, and investment windows aligned with security milestones. Public-private partnerships (PPPs) can marshal private innovation and international funding, bridging capacity gaps; however, they must be governed by strict governance, transparent risk-sharing, and safeguards against external overreach.

Third, a gradual, phased approach is prudent. Instead of a disruptive overhaul, Nigeria should implement a staged roadmap with measurable milestones. Each phase should deliver tangible improvements in security and sovereignty guarantees to attract further investment. This approach builds confidence, distributes financial and technical risk, and creates scalable momentum.

There is also a need to address enforcement amid unauthorised actors. International collaboration is essential because data flows cross borders with ease. A global standards network, drawing on OECD guidelines and the GDPR-inspired practices, can harmonise protections, share threat intelligence, and coordinate enforcement. Strong consequences for cross-border breaches must be clearly defined and enforceable through a cybercrime governance framework akin to an international Interpol for cyber issues. Such collective action ensures deterrence and accountability beyond national borders, preserving data localisation aims.

Emphasis is laid on due diligence for transfers to processors outside Africa. Responsibility rests with data controllers to ensure destination jurisdictions and processors meet established standards. The NDPC should provide explicit adequacy criteria to evaluate recipient jurisdictions, ensuring they have privacy protections and operational safeguards aligned with Nigerian norms. When adequacy is uncertain, contractual clauses, binding corporate rules, and ongoing oversight become essential to maintain data integrity and privacy.

The Nigerian law regulating cross-border data transfers. Under the NDPA and GAID 2025, transfers require clear legal authority, typically via laws, binding corporate rules, contractual safeguards, or certifications. Records and prior notification to the NDPC are mandatory, with the NDPC empowered to assess the adequacy of destination data laws and to designate categories requiring heightened safeguards. Enforcement rests with the NDPC, subject to parliamentary oversight for major policy changes; a notable gap is the absence of an official, published adequacy list of countries, which would improve predictability for investors and partners.

In sum, attracting security-enhancing investments demands a coherent, phased national strategy that treats data sovereignty as a strategic priority, mobilises public and private resources through disciplined PPPs, strengthens international cooperation and enforcement, and clarifies cross-border transfer norms. This balanced approach fosters a secure, scalable data economy capable of withstanding evolving cyber threats while delivering tangible security gains.

Enforcement, Sovereignty, and Practical Challenges

The third speaker, Adanma Isamade, explained that while the NDPA provides an encompassing framework, enforcement remains a significant challenge. The NDPC has the authority to investigate breaches, issue compliance orders, and impose fines ranging up to ₦10 million or 2% of annual turnover for serious violations. However, unlike the European Union, Nigeria has not yet published an official adequacy list of trusted countries, leaving businesses uncertain about permissible destinations for data transfers.

Furthermore, many corporations that process Nigerian data operate without a physical presence in the country, raising questions of enforcement. The webinar highlighted possible solutions, including strengthening regional collaboration through instruments like the Malabo Convention, pursuing bilateral agreements with countries with strong data protection laws to ensure reciprocity and educating Nigerian citizens about their data rights and avenues for redress.

She encouraged data subjects to lodge complaints with the NDPC or by pursuing civil actions in court when their rights are violated.

Next Steps

The webinar session underscored the importance of balance. Nigeria cannot afford to isolate itself with overly rigid localisation laws, as this may stifle innovation and deter foreign investments. At the same time, unrestricted data flows expose citizens to surveillance and exploitation, leading to the loss of control of Nigerians' data by its institutions.

The recommendations from the webinar session include:

- Refining Nigeria's legal framework by issuing clear guidance for cross-border transfer of data.
- Investment in domestic data infrastructure, including data centres and cloud services.
- Foster public-private partnerships that pool expertise and resources.
- The NDPC should engage actively in regional and global conversations on data governance, ensuring African voices shape global norms.

Conclusion

The webinar provided a timely platform to reflect on the complex interplay between innovation and sovereignty in Nigeria's data protection regime. The NDPA 2023 lays a solid foundation, but its success depends on effective enforcement, stakeholder collaboration, and alignment with global best practices.

As Nigeria deepens its participation in the global digital economy, the challenge will be to ensure that data flows drive innovation and growth without undermining citizens' rights or national sovereignty. The discussions underscored that this balance is achievable but only through sustained dialogue, investment, and collective responsibility across government, industry, and civil society.