Cross-Border Data Protection Law: The Nigerian Perspective for International Businesses

+234 (0)702 558 0053
3 Theophilus Orji Street, Off Fola Osibo Road, Lekki Phase 1, Lagos, Nigeria

www.strenandblan.com
contact@strenandblan.com
@strenandblan

Introduction

The quotes, “Data is the new currency” and “Data is King”, aptly represent the growing importance of data as a valuable asset in the 21st century, driving innovation, economic growth and business success. As one of the largest economies in Africa, Nigeria’s strategic position in West Africa and its vast consumer base have inevitably led to multinationals processing the personal data of Nigerian citizens and residents.

From online shopping, social media usage, digital banking, clinical trials, mobile applications, and travel history, to website applications, the personal data of individuals in Nigeria is now being collected and processed daily by multinationals. This constant flow of data across borders gives rise to significant legal, regulatory, and operational obligations within an evolving data protection landscape in Nigeria. The scope of Nigeria’s data protection laws extends beyond entities with a direct presence in the country.

A plethora of compliance obligations exists for multinational corporations collecting and processing personal data of Nigerian citizens and residents, irrespective of non-physical presence in Nigeria. The risks of non-compliance pose serious threats to the stability, reputation, and continuity of operations for multinationals. At **Stren & Blan Partners**, we work closely with international law firms to provide compliance support to their clients operating multinational corporations in Nigeria. Our Firm brings regulatory knowledge, commercial awareness and an ability to anticipate and manage risks in real time, ensuring that global data protection standards are met without losing sight of local realities.

An Overview of Nigeria's Evolving Regulatory Landscape

Nigeria's regulatory environment is undergoing a significant transformation, marked by increased compliance requirements and a growing emphasis on data sovereignty and consumer protection. Regulatory bodies in Nigeria have intensified efforts to create a robust legal framework that governs data protection, cybersecurity, fintech, telecommunications, healthcare and other key sectors.

Agencies such as the Nigeria Data Protection Commission (NDPC), the Federal Competition and Consumer Protection Commission (FCCPC), the Nigerian Communications Commission (NCC) and various sector-specific regulators have adopted a more definitive stance towards ensuring the overall protection of personal data involving Nigerian citizens and residents, including swift responses to perceived breaches. The Courts have equally adopted the same protective stance, affirming the privacy rights of individuals in Nigeria. For multinationals operating in Nigeria, this signals a shift from passive compliance expectations to active regulatory engagement.

This evolving regulatory landscape presents both opportunities and challenges for multinational corporations. While there is growing alignment with international data protection standards such as the General Data Protection Regulation (GDPR), Nigeria's local laws introduce unique considerations, including mandatory filing obligations, local representation requirements, data localization principles, and sector-based compliance protocols. In today's interconnected regulatory ecosystem, a compliance failure in Nigeria can raise flags with regulatory authorities in other jurisdictions, particularly where cross-border data sharing is involved. Multinational entities are now expected to maintain consistent internal standards across all jurisdictions where they operate.

The Nigeria Data Protection Act 2023 (NDPA) emphasizes that cross-border transfers of personal data from Nigeria are only permitted where the recipient country ensures an adequate level of data protection or where appropriate safeguards are in place. In the absence of these, cross-border transfers may still occur with the data subject's explicit consent or if necessary for contractual performance, public interest, or legal claims. Multinational corporations must also maintain documentation of these transfers and ensure transparency, particularly when operating in regulated sectors like finance, healthcare, and telecommunications, where additional sector-specific obligations may apply.

Several recent high-profile enforcement actions underscore the heightened scrutiny facing multinationals in Nigeria. The FCCPC fined META Platforms Inc. and WhatsApp LLC approximately $220 million for violations of consumer protection laws and data privacy standards. The NDPC has recently announced plans to impose substantial fines on data controllers and processors violating the provisions of the Act. Fidelity Bank, a high-profile Nigerian bank, was fined N555 million by the NDPC for violating data privacy regulations. These enforcement actions reflect a maturing regulatory landscape, one that is not only more coordinated but also more assertive in enforcement.

Sector-Specific Risk Realities for Multinationals in Nigeria

Multinational corporations controlling or processing data of Nigerian citizens or persons resident in Nigeria face regulatory exposures, particularly when compliance gaps arise in cross-border data transfers. These risks often materialize from how regulatory frameworks are interpreted, applied, and enforced across different sectors. The following sectoral breakdown highlights the regulatory risks multinationals must navigate in the data collection and processing of personal data of Nigerian citizens and residents:

1. Financial Sector:

The financial sector remains one of the most highly scrutinized environments for multinationals. Multinational banks, fintechs, and payment platforms operating in Nigeria are under dual scrutiny from both the NDPC and the Central Bank of Nigeria (CBN). The CBN mandates strict controls around customer data, Know Your Customer (KYC) records, and transaction histories. Data localization is particularly sensitive in this sector, with an expectation that critical financial data is hosted onshore or on approved cloud platforms with local counterparts. Notably, the increasing use of fintech platforms has added another layer of regulatory complexity, especially where digital wallets, virtual assets, and data protection obligations intersect.

2. Health and Pharmaceuticals Sector:

Multinationals operating within the healthcare and pharmaceutical sector, conducting clinical trials in Nigeria or utilizing personal data of Nigerian citizens and residents, can be vulnerable to data breaches involving sensitive patient information and violations of the local regulations. Patient health records, biometrics, and genetic information are considered highly sensitive personal data and utmost compliance levels are expected. Express prior informed consent must be obtained for data processing. Data breaches within the healthcare sector can result in reputational damage, physical harm, and death, highlighting the need for strict data protection measures. Data protection regulations within the sector emphasize confidentiality, security and transparency principles. Foreign companies are increasingly expected to implement rigorous compliance protocols to ensure all local subsidiaries, distributors, and research partners adhere to national health and safety laws. Additional approvals may be required from the Federal Ministry of Health and other ethics boards for data transfers.

3. Technology and Telecommunications:

Multinationals operating within this sector face risks related to cyber impersonation, unauthorised data collection, unlawful sharing or sale of consumer data. Misuse of personal data for targeted marketing campaigns has become a focal point for regulators. The NCC creates additional licensing frameworks and requirements for compliance, which require strict adherence to adequacy standards, encryption protocols, and user consent structures. With the growing emphasis on data privacy, the violation of the NDPA and NCC can result in grave sanctions.

4. Retail and E-Commerce:

Retail and digital commerce platforms are booming in Nigeria, but so are the associated data protection compliance risks. Global retail brands and e-commerce platforms, whether through online marketplaces, apps, or physical stores, regularly collect and process consumer data, including purchase history, financial details, behavioural analytics, and delivery addresses. Multinationals are faced with compliance risks where personal data of Nigerian citizens and residents is collected and processed via such platforms. Foreign retailers or platforms face growing exposure to mishandling of customer data and violation of privacy rights, especially where such data is transferred across borders. The FCCPC and NDPC are increasingly coordinating efforts to hold e-commerce platforms accountable for data protection violations, including data monetization and third-party advertising, and actions of their third-party sellers, payment facilitators, and logistics providers.

5. Travel and Hospitality

Multinational airlines, hotel chains, travel agencies, and booking platforms handle large volumes of highly sensitive Personally Identifiable Information (PII), including passport data, travel itineraries, payment information, and even biometric data for identity verification. These datasets often flow across borders for purposes such as global reservation management, customer profiling, and loyalty program administration. Under the NDPA, such transfers must meet strict conditions: a lawful basis for processing, data subject consent, and adequate safeguards for cross-border movement. Additionally, hospitality operators must navigate cybersecurity expectations around the protection of guest data and surveillance systems (e.g., CCTV). Given the industry's high exposure to cyber threats and identity fraud, the NDPC expects entities in this space to implement robust encryption, access control, and breach response plans. Failure to align with data minimization and privacy-by-design principles can lead to enforcement actions and reputational risk.

Compliance Measures and Strategies

In Nigeria's fast-evolving regulatory environment, multinational companies must adopt comprehensive and adaptable compliance strategies to ensure alignment with data protection laws in Nigeria. The most resilient businesses are those that embed compliance into their operational culture, aligning local legal obligations with global standards.

1. Data Mapping and Classification:

An effective compliance strategy begins with understanding the data lifecycle within the organization. This includes conducting thorough data mapping exercises to identify what personal data is collected, where it is stored, how it is processed, and with whom it is shared. Proper classification helps determine applicable legal obligations and risk levels, which is essential to develop localised compliance frameworks.

2. Local Registration, Representation and Regulatory Filings:

Multinationals processing data of Nigerian citizens and residents may be required to register with the NDPC. Additionally, the NDPC requires the appointment of a Data Protection Officer (DPO), irrespective of physical presence in Nigeria, where the data controller or processor is involved in the collection or processing of the personal data of data subjects in Nigeria and meets the thresholds for significant data processing activities as defined by the Commission, including large-scale processing, sensitive personal data handling, or operations that present high risks to the rights and freedoms of individuals. Additionally, entities are required to file data protection reports detailing data processing audits and undertake annual compliance audits.

3. Policy Development and Implementation:

Multinationals should develop and regularly update internal policies pertaining to data protection, information security, consent management, and breach notification protocols. These policies should be tailored to comply with the NDPA and relevant sectoral regulations.

4. Employee Training and Awareness:

Data protection training and awareness programs for employees and staff are necessary to mitigate risks of violations of data protection principles, regulatory expectations, and internal compliance protocols. Regular training sessions help embed a culture of compliance across all operational levels.

5. Regulatory Engagement and Risk Assessment:

Proactive engagement with regulators such as the NDPC and FCCPC helps multinationals stay ahead of enforcement trends and regulatory expectations. Regular risk assessments should also be conducted to identify compliance gaps and emerging legal risks in a fast-changing regulatory environment.

6. Incident Response and Breach Management:

The NDPC requires mandatory incident breach reporting, hence, multinationals must establish clear incident response frameworks for managing data breaches or regulatory breaches. This includes notification procedures, containment protocols, and documentation of corrective actions in line with statutory requirements.

Furthermore, continuous risk assessment remains essential. Companies must conduct regular internal audits, leverage automated compliance tracking tools where possible, and maintain robust data protection frameworks. These measures help to proactively identify and address emerging privacy risks, ensuring ongoing vigilance against data violations. Regulatory engagement and transparency go a long way in building credibility. Companies must invest in digital and operational resilience. Regular penetration testing, access control enforcement, and cyber-attack readiness assessments help to mitigate data breaches.

Conclusion

As data protection expectations rise globally and within Nigeria, multinationals collecting and processing personal data of Nigerian citizens and residents must treat compliance as a core business function, not an afterthought. With targeted audits, compliance frameworks, sector-specific controls, and proactive engagement with regulators, multinationals will not only minimise legal exposure but also build lasting credibility and resilience in Nigeria, one of Africa's most dynamic markets.

Our Role as Local Counsel

At Stren & Blan Partners, we regularly support international firms and their clients in assessing regulatory exposure, conducting data compliance audits, offering strategic advice, liaising with regulatory authorities, and establishing sustainable data protection compliance mechanisms tailored to Nigerian realities. Our Firm is committed to working with international law firms and their clients to deliver solutions that are both locally attuned and globally compliant. Whether managing internal audits, setting up compliance frameworks or providing forward-looking compliance advisory, we remain a trusted advisor in fostering regulatory resilience in Nigeria.

About Stren & Blan Partners

Stren & Blan Partners is an innovative and dynamic Law Firm with a compelling blend of experienced lawyers and energetic talents. We are focused on providing solutions to our client's business problems and adding value to their businesses and commercial endeavours. This underpins our ethos as everything we do flows from these underlying principles.

Stren & Blan Partners is a full-service commercial Law Firm that provides legal services to diverse local and multinational corporations. We have developed a clear vision for anticipating our client's business needs and surpassing their expectations, and we do this with an uncompromising commitment to Client service and legal excellence.

Contact Persons

Christian Aniukwu
Partner
ChristianAniukwu
@strenandblan.com

Francisca Igboanugo
Team Lead
FranciscaIgboanugo
@strenandblan.com

Chizoba Anyaeji
Associate
ChizobaAnyaeji
@strenandblan.com

+234 (0)702 558 0053
3 Theophilus Orji Street, Off Fola Osibo Road, Lekki Phase 1,
Lagos, Nigeria

www.strenandblan.com
contact@strenandblan.com
@strenandblan